

**UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA**

Jennie Marie Loeffler,

File No. 13-cv-2060 (MJD/TNL)

Plaintiff,

v.

**REPORT &
RECOMMENDATION**

City of Anoka; City of Burnsville; Dakota County; Dakota County Communications Center; City of Duluth; City of Eagan; City of Fairmont; City of Farmington; City of Hancock; Isanti County; Mille Lacs County; City of Minneapolis; City of Morris; Renville County; Rice County; City of Richfield; City of Roseville; City of St. Francis; City of St. Paul; City of Staples; Wright County; Yellow Medicine County; Michael Campion, acting in his individual capacity as Commissioner of the Minnesota Department of Public Safety; Ramona Dohman, acting in her individual capacity as Commissioner of the Minnesota Department of Public Safety; John and Jane Does (1-30), acting in their individual capacity as officers, supervisors, staff, employees, independent contractors or agents of the Minnesota Department of Public Safety; Entity Does (1-50), including cities, counties, municipalities, and other entities sited in Minnesota departments and agencies; A Female Officer to be Later Named, Acting in Her Individual Capacity as a Law-Enforcement Officer for the City of Duluth; City of Lakeville; City of Mankato; City of Milaca; City of New Prague; City of Pequot Lakes; and Saint Louis County,

Defendants.

Kenneth H. Fukuda, Lorenz F. Fett, Jr., Mark H. Zitzewitz, Sonia L. Miller-Van Oort, and Jonathan A. Strauss, Sapiaientia Law Group PLLC, 12 South Sixth Street, Suite 1242, Minneapolis, MN 55402 (for Plaintiff);

Jon K. Iverson, Stephanie A. Angolkar, and Susan M. Tindal, Iverson Reuvers Condon, 9321 Ensign Avenue South, Bloomington, MN 55438 (for Defendants Cities of Anoka, Burnsville, Eagan, Fairmont, Farmington, Hancock, Lakeville, Mankato, Milaca, Morris, New Prague, Pequot Lakes, Richfield, Roseville, St. Francis, and Staples and Dakota County Communications Center);

Andrea G. White, Assistant County Attorney, Dakota County Attorney's Office, 1560 Highway 55, Hastings, MN 55033 (for Defendant Dakota County);

M. Alison Lutterman, Deputy City Attorney, and Nathan N. LaCoursiere, Assistant City Attorney, Duluth City Attorney's Office, 411 West First Street, 410 City Hall, Duluth, MN 55802 (for Defendant City of Duluth);

Jamie L. Guderian and Joseph E. Flynn, Jardine Logan & O'Brien PLLP, 8519 Eagle Point Boulevard, Suite 100, Lake Elmo, MN 55042 (for Defendants Isanti, Mille Lacs, Renville, Rice, Wright, and Yellow Medicine Counties); and

Oliver J. Larson, Assistant Attorney General, Minnesota Attorney General's Office, 445 Minnesota Street, Suite 1800, St. Paul, MN 55101-2134 (for Defendants Commissioners Michael Campion and Ramona Dohman).

I. INTRODUCTION

This matter is before the Court, United States Magistrate Judge Tony N. Leung, on multiple motions to dismiss: Commissioners Michael Campion and Ramona Dohman's Motion to Dismiss (ECF No. 19); County of Dakota's Motion to Dismiss (ECF No. 33); Motion to Dismiss of Defendants Isanti County, Mille Lacs County, Renville County, Rice County, Wright County and Yellow Medicine County (ECF No. 39); Defendant City of Duluth's Motion to Dismiss Pursuant to Fed. R. Civ. P. 8(a)(2) and 12(b)(6) (ECF No. 49); and Cities of Anoka, Burnsville, Eagan, Fairmont, Farmington, Hancock,

Lakeville, Mankato, Milaca, Morris, New Prague, Pequot Lakes, Richfield, Roseville, St. Francis, and Staples and Dakota County Communications Center’s Motion to Dismiss (ECF No. 53). These motions have been referred to the undersigned magistrate judge for a report and recommendation to the district court, the Honorable Michael J. Davis, Chief District Judge of the United States District Court for the District of Minnesota, under 28 U.S.C. § 636 and Local Rule 72.2(b). (ECF Nos. 27, 38, 46, 61.)

A hearing was held. Kenneth H. Fukuda and Sonia L. Miller-Van Oort appeared on behalf of Plaintiff. (ECF No. 78.) Susan M. Tindal appeared on behalf of Defendants Cities of Anoka, Burnsville, Eagan, Fairmont, Farmington, Hancock, Lakeville, Mankato, Milaca, Morris, New Prague, Pequot Lakes, Richfield, Roseville, St. Francis, and Staples and Dakota County Communications Center (“Cities”). (*Id.*) Andrea G. White appeared on behalf of Defendant County of Dakota (“Dakota County”). (*Id.*) M. Alison Lutterman appeared on behalf of Defendant City of Duluth (“Duluth”). (*Id.*) Joseph E. Flynn appeared on behalf of Defendants Isanti, Mille Lacs, Renville, Rice, Wright, and Yellow Medicine Counties (“Counties”). (*Id.*) Oliver J. Larson appeared on behalf of Defendants Commissioners Michael Campion and Ramona Dohman (“Commissioners”). (*Id.*)

Based upon the record, memoranda, and the proceedings herein, **IT IS HEREBY RECOMMENDED** that (1) Commissioners Michael Campion and Ramona Dohman’s Motion to Dismiss (ECF No. 19) be **GRANTED**; (2) County of Dakota’s Motion to Dismiss (ECF No. 33) be **GRANTED**; (3) Motion to Dismiss of Defendants Isanti County, Mille Lacs County, Renville County, Rice County, Wright County and Yellow

Medicine County (ECF No. 39) be **GRANTED**; (4) Defendant City of Duluth's Motion to Dismiss Pursuant to Fed. R. Civ. P. 8(a)(2) and 12(b)(6) (ECF No. 49) be **GRANTED IN PART** and **DENIED IN PART**; and (5) Cities of Anoka, Burnsville, Eagan, Fairmont, Farmington, Hancock, Lakeville, Mankato, Milaca, Morris, New Prague, Pequot Lakes, Richfield, Roseville, St. Francis, and Staples and Dakota County Communications Center's Motion to Dismiss (ECF No. 53) be **GRANTED**.

II. BACKGROUND¹

Plaintiff brings claims under the Driver's Privacy Protection Act ("DPPA"), 18 U.S.C. § 2721 *et seq.*; 42 U.S.C. § 1983; and state common law based on accesses of her personal and private driver's license information. (Compl. ¶¶ 6, 179-205, 224-77, ECF No. 1.) This action is one of several actions recently filed in this District alleging unlawful access of private data. *See, e.g., Kiminski v. Hunt*, File No. 13-cv-185 (JNE/TNL) (consolidated cases); *Kost v. Hunt*, File No. 13-cv-583 (JNE/TNL); *Potocnik v. Anoka Cnty.*, File No. 13-cv-1103 (DSD/TNL) (Ltr. to Hon. Michael J. Davis, Mar. 25, 2014, listing pending DPPA cases (ECF No. 98)).

A. The Database & Records Maintained

The Driver and Vehicle Services Division ("DVS") of the Minnesota Department of Public Safety ("DPS") maintains a database containing the motor vehicle records of

¹ "In analyzing a motion to dismiss, a court must accept the allegations contained in the complaint as true and make all reasonable inferences in favor of the nonmoving party." *Martin v. Iowa*, ___ F.3d ___, 2014 WL 2013965, at *1 (8th Cir. 2014); *see also Rasmusson v. Chisago Cnty.*, No. 12-cv-0632 (SRN/JSM), ___ F. Supp. 2d ___, 2014 WL 107067, at *2 (D. Minn. Jan. 10, 2014) ("When evaluating a motion to dismiss, the Court assumes the facts in the Complaint to be true and construes all reasonable inferences from those facts in the light most favorable to Plaintiff.").

Minnesota drivers, including Plaintiff.² (Compl. ¶¶ 63, 97-99.) The database contains information including but not limited to drivers' names, dates of birth, license numbers, addresses, license photos, physical descriptions (weight, height, and eye color), Social Security numbers, and health and disability information. (*Id.* ¶ 64.)

“The DPPA regulates the disclosure of personal information contained in the records of state motor vehicle departments (DMVs).” *Maracich v. Spears*, 133 S. Ct. 2191, 2195 (2013). Under the DPPA, “information that identifies an individual, including an individual’s photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information” is considered “personal information.” 18 U.S.C. § 2725(3). The DPPA further categorizes “an individual’s photograph or image, social security number, medical or disability information” as “highly restricted personal information.” *Id.* § 2725(4). In general, the DPPA prohibits the disclosure and use of personal information and highly restricted personal information obtained in connection with a motor vehicle record unless accessed for certain permissible uses. *Id.* §§ 2721(a), (b), 2722(a); *Maracich*, 133 S. Ct. at 2195 (“Disclosure of personal information is prohibited unless for a purpose permitted by an exception listed in 1 of 14 statutory subsections.”); *Kiminski v. Hunt*, File Nos. 13-cv-185 (JNE/TNL), 13-cv-389 (JNE/TNL), 13-cv-208 (JNE/TNL), 13-cv-358 (JNE/TNL), 13-cv-286 (JNE/TNL), 2013 WL 6872425, at *3 (D. Minn. Sept. 20, 2013) (“The DPPA generally restricts state departments of motor

² There appear to be two different databases that contain driver’s license information: the database maintained by DVS and a database maintained by the Bureau of Criminal Apprehension. (Compl. ¶ 51; *see also id.* ¶¶ 56, 167.) Plaintiff appears to allege that the impermissible access of her private data took place through the DVS database. (*See* Compl. ¶¶ 63-65, 97-102.) Therefore, the Court uses “database” in the singular.

vehicles . . . , other organizations, and individuals from disclosing personal information contained in motor vehicle records except as allowed for under the statute.”).

B. Accesses of Plaintiff’s Information

For approximately 17 years, until December 2012, Plaintiff was married to a law-enforcement officer with Defendant City of Lakeville. (Compl. ¶¶ 52, 59.) Plaintiff’s then-husband worked for several police departments during their marriage and continues to be employed by Defendant City of Lakeville. (*Id.* ¶ 53.) At some point during their marriage, Plaintiff’s then-husband had an affair with Defendant Female Officer to be Later Named (“Defendant Female Officer”), who was a law-enforcement officer with Defendant City of Duluth. (*Id.* ¶¶ 54, 55.) Plaintiff confronted Defendant Female Officer about the affair on September 30, 2009. (*Id.* ¶ 55.)

Around May 2011, Plaintiff became concerned that her private data had been impermissibly accessed and contacted DPS, “requesting that DPS determine and advise her if any individuals were accessing her personal and private driver’s license information” through the database. (*Id.* ¶ 56.) Plaintiff was told that such information “could not be provided to [her] unless she had a specific reason for requesting that information.” (*Id.* ¶ 57.) At the time, this ended Plaintiff’s inquiry because she believed such information would not be provided to her given that (1) “she was not positive that her information had been impermissibly accessed” and (2) she was unsure “she had a reason for requesting that information as required by the DPS.” (*Id.* ¶ 58.)

In 2013, after seeing media coverage of an individual whose personal information had been impermissibly accessed by law enforcement personnel in Minnesota, Plaintiff

again contacted DPS to request information regarding access of her driver's license information. (*Id.* ¶ 60.) DPS told Plaintiff that it would audit her information and, approximately one week later, provided Plaintiff an audit related to accesses of her driver's license information from 2003 through 2013. (*Id.* ¶ 62.) Plaintiff's driver's license information was viewed more than 130 times over this ten-year period. (*Id.* ¶ 2.)

C. Litigation

Plaintiff filed the instant litigation on July 30, 2013. (Compl.) In Count I, Plaintiff alleges all Defendants violated the DPPA. (*Id.* ¶¶ 179-205.) In Count II, Plaintiff alleges that certain individual Defendants violated her rights under the Fourth and Fourteenth Amendments and 42 U.S.C. § 1983. (*Id.* ¶¶ 206-23.) In Count III, Plaintiff alleges that the entity Defendants (including the Cities, Duluth, the Counties, and Dakota County) were aware of the widespread access of private data for personal use; such use was against regulations promulgated by the entity Defendants; and the entity Defendants' pervasive failure to take action to stop or prevent such use (including the failure to properly train, monitor, supervise, and properly discipline) amounted to deliberate indifference to Plaintiff's rights, all in violation of 42 U.S.C. § 1983. (*Id.* ¶¶ 224-246.) In Count IV, Plaintiff alleges that the Commissioners were responsible for creating, maintaining, and providing access to the database containing Plaintiff's private data; had the ability to prevent unauthorized access to Plaintiff's private data; and failed to prevent such unauthorized access despite that they knew or should have known such access was occurring, thereby demonstrating deliberate indifference to Plaintiff's rights in violation of 42 U.S.C. § 1983. (*Id.* ¶¶ 247-63.) Relatedly, in Count V, Plaintiff seeks

prospective relief under 42 U.S.C. § 1983 against Commissioner Dohman permanently enjoining the unauthorized access of private data and requiring the establishment of policies, practices, and procedures to prevent such unauthorized access of private data. (*Id.* ¶¶ 264-71.) Finally, in Count VI, Plaintiff alleges all Defendants invaded her privacy under common law. (*Id.* ¶¶ 272-77.)

III. MOTIONS TO DISMISS

The defendants identified above have all moved for dismissal pursuant to Fed. R. Civ. P. 12(b)(6) for “failure to state a claim upon which relief can be granted.” “To withstand a Rule 12(b)(6) motion, a complaint must contain sufficient factual allegations to ‘state a claim to relief that is plausible on its face.’” *Smithrud v. City of St. Paul*, Nos. 12-3713, 12-3736, 746 F.3d. 391, 397 (8th Cir. 2014) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 547 (2007)). “[A]lthough a complaint need not contain ‘detailed factual allegations,’ it must contain facts with enough specificity ‘to raise a right to relief above the speculative level.’” *United States ex rel. Raynor v. Nat’l Rural Utils. Coop. Fin., Corp.*, 690 F.3d 951, 955 (8th Cir. 2012) (quoting *Twombly*, 550 U.S. at 555); *see also Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (“[T]he pleading standard Rule 8 announces does not require ‘detailed factual allegations,’ but it demands more than an unadorned, the-defendant-unlawfully-harmed-me accusation.”). “A pleading that offers ‘labels and conclusions’ or ‘a formulaic recitation of the elements of a cause of action will not do.’” *Iqbal*, 556 U.S. at 678. Similarly, “[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice.” *Id.* “In deciding a motion to dismiss under Rule 12(b)(6), a court assumes all facts in the

complaint to be true and construes all reasonable inferences most favorably to the complainant.” *Raynor*, 690 F.3d at 955.

A. Commissioners³

1. DPPA

With respect to the Commissioners, Plaintiff focuses on their role in creating and maintaining the database. Plaintiff alleges that the Commissioners knowingly created the database containing Plaintiff’s private data and granted law-enforcement personnel access to the database. (Compl. ¶¶ 97, 99.) Plaintiff alleges that the Commissioners had the ability to monitor access to and prevent unauthorized access of the database and failed to prevent unauthorized access. (*Id.* ¶¶ 100-02.) In doing so, Plaintiff alleges that the Commissioners knowingly disclosed her private data and were aware that law-enforcement personnel were viewing her private data. (*Id.* ¶¶ 103, 108-10, 122.) Plaintiff alleges that the Commissioners knowingly disclosed Plaintiff’s private data by granting access to the database, thus violating the DPPA, “even if they did not know that the Defendant Individuals accessed and obtained the information for an impermissible purpose.” (*Id.* ¶ 194.) Plaintiff alleges that the Commissioners were reckless and grossly negligent in their supervision of subordinate employees who operated the database. (*Id.* ¶¶ 129-30.) Further, Plaintiff alleges that the Commissioners knew law-enforcement personnel were accessing the database for impermissible purposes. (*Id.* ¶¶ 121, 163-75.)

³ As stated in II(C) *supra*, Plaintiff also brings a common-law, invasion-of-privacy claim against the Commissioners (Count VI). (Compl. ¶¶ 272-77.) Plaintiff correctly points out that the Commissioners have not moved to dismiss this claim, (Pl.’s Mem. in Opp’n to Comm’rs. at 43 n.11, ECF No. 30), and, as a result, the Court has not considered the sufficiency of this claim as it relates to the Commissioners.

The Commissioners assert that Plaintiff has failed to state a claim under the DPPA because creation and maintenance of the database alone is not actionable under the DPPA, and simply granting access to the database does not make them accountable for misuse of Plaintiff's private data by others. (Commrs' Mem. in Supp. at 6, 7-8, ECF No. 20.) The Commissioners contend that "Plaintiff does not allege that either Commissioner personally obtained, disclosed, or used her driver's license data, let alone for a 'purpose not permitted.'" (*Id.* at 6.) Additionally, the Commissioners assert that, even if the knowledge of misuse of private data would support a DPPA claim against the Commissioners, Plaintiff has not sufficiently pleaded facts alleging the Commissioners' knowledge of such misuse. (*Id.* at 8-10.)

a. Creation & Maintenance Of & Grants of Access To

The Commissioners' first argument—that they cannot be held liable under the DPPA for their roles in creating, maintaining, and granting access to the database—highlights a central issue in DPPA litigation: whether the use of "knowingly" in § 2724(a) modifies just the act of disclosure or also applies to the purpose for the disclosure. Under the DPPA, "[a] person who *knowingly* obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under [the DPPA] shall be liable to the individual to whom the information pertains, who may bring a civil action in a United States district court." 18 U.S.C. § 2724(a) (emphasis added). Arguably, if "knowingly" applied only to the act of disclosure, the Commissioners would face liability under the DPPA anytime the database is misused based simply on their involvement in the creation and maintenance of and grants of access to the database.

Plaintiff advocates for just such a construction, arguing that the DPPA prohibits *any* release or access of information unless the disclosure is for a specific permissible purpose. (Pl.’s Mem. in Opp’n to Commrs. at 8, ECF No. 30.) Plaintiff argues that “if the Commissioners knowingly disclosed the information, and it was not obtained for a ‘government use,’ the fact that [the Commissioners] did not know of the misuse is irrelevant to civil liability.” (*Id.* at 11.) Plaintiff asserts that “[n]either *personally* disclosing, nor *actual* knowledge, nor *knowledge of improper purpose*, nor any of the Defendant Personnel as *the intended recipient*, nor of *their misuse* is required by the statute.” (*Id.* at 15.) Plaintiff contends that, as the individuals who made the database—and consequently, Plaintiff’s private data—available to others, the Commissioners owed some duty of care in their release of Plaintiff’s private data. (*See id.* at 15-24.)

The courts in this District that have considered whether the Commissioners’ roles in creating, maintaining, and granting access to the database state a claim under the DPPA have all concluded that the acts of making a plaintiff’s private data available via the database are insufficient. “To plead a valid DPPA claim against the Commissioners, [a plaintiff] must plausibly allege not only that the Commissioners knowingly disclosed her information, but also that the Commissioners had an impermissible purpose in doing so.” *Potocnik v. Carlson*, No. 13-cv-2093 (PJS/JJG), ___ F. Supp. 2d ___, 2014 WL 1206403, at *5 (D. Minn. March 24, 2014). “[T]he DPPA does not impose liability on one who indirectly facilitates another’s access of a motor vehicle record by maintaining an electronic database.” *Bass v. Anoka Cnty.*, No. 13-cv-860 (DSD/JJG), ___ F. Supp. 2d ___, 2014WL 683969, at *3 (D. Minn. Feb. 21, 2014); *accord Gulsvig v. Mille Lacs*

Cnty., 13-cv-1309 (JRT/LIB), 2014 WL 1285785, at *5 (D. Minn. March 31, 2014) (“[T]he text of the [DPPA] limits liability to those who disclose, use, access, or obtain information themselves for an impermissible purpose, not those who provide access to information that is *subsequently* used for an impermissible purpose.”); *Nelson v. Jesson*, No. 13-cv-340 (RHK/JJK), 2013 WL 5888235, at *3 (D. Minn. Nov. 1, 2013) (“It is not enough that [the Commissioners] disclosed information to Schlener and *he* acted with an impermissible purpose, the Commissioners *themselves* must have acted with such a purpose.”); *see also Cook v. ACS*, 663 F.3d 989, 994 (8th Cir. 2011) (“The proper focus for courts is not the manner in which the information was acquired, but the use to which it is eventually put.”); *Kiminski*, 2013 WL 6872425, at *6 (“If the person discloses the information for a permissible purpose, the plain language of the provision does not make the person liable for a subsequent misuse by the recipient.”).

Plaintiff contends that that “[t]he Commissioners exercised no care in releasing the information—by issuing passwords—to the individual officers and other non-government employees who have violated Plaintiff’s rights.” (Pl.’s Mem. in Opp’n to Commrs. at 21.) Plaintiff asserts that the Commissioners “exact no specific permissible purpose from the end user; they do not monitor usage; they do not train; they do nothing whatsoever but assume [individuals] will all use [the database] correctly.” (*Id.* at 21-22.) But as aptly described by another court in this District, “in reality, Plaintiff’s allegations amount to a claim that the Commissioner Defendants violated the DPPA by releasing the information to their respective employees and agencies for a *permitted purpose* (i.e., doing their jobs), *but without* proper safeguards, training, or monitoring. This is not the

same as releasing the information for an impermissible purpose.” *Mallak v. Aitkin Cnty.*, No. 13-cv-2119 (DWF/LIB), ___ F. Supp. 2d ___, 2014 WL 1285807, at *15 (D. Minn. Mar. 31, 2014).

Further, courts in this District have rejected the idea that the Commissioners owe a duty of care under the DPPA or *Gordon v. Softech International Inc.*, 726 F.3d 42 (2d Cir. 2013). Looking to the plain language of the DPPA, these courts have held that § 2724(a)’s “*knowingly* obtains, discloses or uses” requirement is not compatible with a duty-of-reasonable-care/negligence standard. *See Gulsvig*, 2014 WL 1285785, at *6 (“But the Act’s *mens rea* requirement is ‘*knowingly*,’ not negligence, 18 U.S.C. § 2724(a) (emphasis added), and nothing in the Act suggests that the Act imposes a reasonable duty of care to safeguard information subject to the Act.”); *Kiminski*, 2013 WL 6872425, at *9 (“[T]he plain language of the civil action provision of the DPPA limits its applicability to a person who knowingly obtained, disclosed, or used personal information for an impermissible purpose. . . . [T]he provision may not be stretched to the point of rewriting it so it reaches others at a state agency who gave the officer database access for a legitimate purpose, merely because they did so in a negligent manner.”). They have rejected plaintiffs’ attempts to bring private causes of action for alleged mismanagement of private data. *See Bass*, 2014 WL 683969, at *3 (“Moreover, unlike other statutes, the DPPA does not expressly create a private right of action for mismanagement of records, and the court declines to recognize one here.”); *see also Potocnik*, 2014 WL 1206403, at *6 (“But nothing in the DPPA explicitly or implicitly imposes a privately enforceable duty to use reasonable care on the states.”)

Indeed, a separate provision of the DPPA addresses state departments of motor vehicles with “a policy or practice of substantial noncompliance[,] . . . subject[ing them] to a civil penalty imposed the Attorney General.” 18 U.S.C. § 2723(b); *see* 18 U.S.C. § 2725(2) (excluding states and their agencies from definition of “person” under DPPA); *Kiminski*, 2013WL 6872425, at *8 (“This provision for sanctions by the Attorney General indicates that Congress intended to address the concern that Plaintiffs attempt to raise here—of inadequate policies and practices at state DMVs to protect the privacy of drivers’ personal information—via that mechanism.”); *see also Potocnik*, 2014 WL 1206403, at *6 (“Taken together, [the private-cause-of-action and state DMV] provisions quite clearly indicate that Congress did not intend to impose a duty of reasonable care on state agencies that would be enforceable in private litigation.”). “[I]t may be true that the Commissioners have not used reasonable care to prevent misuse of the DVS database. . . . [But] the DPPA does not impose a duty of care on the Commissioners.” *Potocnik*, 2014 WL 1206403, at *6.

In *Gordon*, the Second Circuit held that “resellers are subject to a duty of reasonable care before disclosing DPPA-protected personal information.” 726 F.3d at 56-57; *see also id.* at 53. *Gordon* involved a chain of entities: (1) a data broker who had access to state motor vehicle records and with whom other entities could contract in order to access the private data; (2) a contracting private-investigative service; and (3) an information-retrieval service owned by the private-investigative service. *Id.* at 45, 46. Because the private-investigative service and its information-retrieval service did not have access to the private data themselves, requests for information were relayed “up the

chain” to the data broker who obtained the information. *Id.* at 46. The information was then relayed “down the chain” to the requester. *Id.* In connection with this process, representations were made concerning the requester’s use for the information. *Id.* As part of its contract, the private-investigative service “represent[ed] that it, and to the extent that it resells this information, any end user will use the information in a manner permitted by law.” *Id.* The information-retrieval service required the requester to specify a purpose for the requested information from a dropdown menu of purposes the information-retrieval service had deemed permissible under the DPPA. *Id.*

In its analysis, the Second Circuit expressly recognized that “[t]he DPPA does not explicitly provide for a duty of reasonable care.” *Id.* at 55. Looking to the DPPA’s legislative history, the Second Circuit concluded that “in light of the clear congressional intent to safeguard the privacy and safety of drivers, it is inconceivable that a dropdown menu, a check box, and a representation that no laws would be violated could satisfy any reasonable diligence floor.” *Id.* at 56. Significantly, in finding that such resellers owed a duty of reasonable care before disclosing private data, the Second Circuit explicitly distinguished a decision from the Sixth Circuit, *Roth v. Guzman*, involving disclosure by a state department of motor vehicles wherein “the Sixth Circuit concluded that a state DMV was not subject to civil liability under the DPPA unless it actually knew that the recipient, who had represented that it had a permissible use for the requested DPPA-protected personal information, would use it for an improper purpose.” *Id.* at 55 (citing

650 F.3d 603, 611-12 (6th Cir. 2011)).⁴ The Second Circuit also explicitly limited its holding to private resellers. *Id.* at 57 n.14 (“Notwithstanding the similarities among upstream sources of DPPA-protected information, as this case does not require us to consider the effect on state DMVs, we limit our holding to private resellers under the statute.”).

While Plaintiff urges this Court to import *Gordon*’s duty of care here, this Court—like those before it—is not persuaded. First, the Second Circuit directly communicated the narrowness of its holding. *Id.*; *see also Kiminski*, 2013 WL 6872425, at *8 (“The Second Circuit explicitly limited its holding in *Gordon* to resellers—private intermediaries who sell data obtained from state DMVs—and noted that the court had not conducted an analysis to make its determination more generally applicable.”). Second, this Court agrees with the reasoning of the *Potocnik* and *Gulsvig* courts, which focused on the factual distinction between state creation and maintenance of a repository of information for its own use and those who resell that information:

The Commissioners did not sell information on the open market (or if they did, that is not the basis of Potocnik’s claim). Instead, the Commissioners created a password-protected database for a specific population of law-enforcement officers and other users who have many and

⁴ Indeed, the Sixth Circuit observed:

If no distinction is made between the use for which the *defendants disclosed* the information, and the undisclosed use for which it was obtained, subsequently misused or impermissibly redisclosed by the recipient, the DPPA becomes essentially a strict liability statute. Every subsequent misuse could be traced back to a violation by the state official. Rather than place all of the liability with the state officials, however, the DPPA makes it unlawful for any person (excluding states and their agencies) to knowingly obtain, disclose, or use the information for a purpose not permitted by the DPPA.

Roth, 650 F.3d at 611. The same reasoning is applicable to the Commissioners.

frequent legitimate uses for the information. *Gordon* therefore does not persuade the Court that state governments owe a federally imposed duty of care in creating and maintaining driver's-license databases. (The Second Circuit may not disagree; it quite explicitly limited its holding to private resellers.)

Potocnik, 2014 WL1206403, at *7 (citation omitted); accord *Gulsvig*, 2014 WL 1285785, at *6 n.4 (“The [*Gordon*] court’s reasoning operated under the facts in that case—a reseller disclosing to an end-user—which are distinct from those here—a state DPS Database being available to state and county law enforcement employees. Given this difference and the plain language of the statute, the Court declines to read a reasonable duty of care into the statute, particularly with regard to the Commissioner Defendants here.”); see also *Mallak*, 2014 WL 1285807, at *16 (relying on *Kiminski* and concluding “that *Gordon* is inconsistent with the plain language of the DPPA and the Commissioner Defendants cannot be held individually liable for systemic issues as alleged in the complaint”).

Therefore, to the extent Plaintiff alleges that the Commissioners are liable under the DPPA for their roles in creating, maintaining, and granting access to the database, Plaintiff fails to state a claim upon which relief can be granted.

b. Disclosure for a Purpose Not Permitted

The Commissioners also move for dismissal on the basis that Plaintiff has not alleged that they personally disclosed her private data or that any disclosure was for a purpose not permitted. (Comms. Mem. in Supp. at 2, 6.)

“To state a claim under the DPPA, a plaintiff must allege that: (1) a defendant knowingly obtained, disclosed or used personal information; (2) from a motor vehicle record; (3) for a purpose not permitted.” *Mallak*, 2014 WL 1285807, at *6. Plaintiff does not allege that the Commissioners personally accessed her private data. (*See* Compl. ¶¶ 66-94.) Rather, the acts of disclosure alleged in the Complaint are the creation and maintenance of and grants of access to the database. (*Id.* ¶¶ 97-99, 108-110, 111-12, 187; *see id.* ¶¶ 103, 192-94.) As already discussed, the Commissioners’ acts in creating, maintaining, and making available a database of private information are not actionable under the DPPA. Further, the number of permissible uses for which private data may be disclosed demonstrates more than tacit approval by Congress that such information may be collected and aggregated in the first place. *See* 18 U.S.C. §2721(b) (listing permissible uses); *Cook*, 663 F.3d at 995 (“One co-sponsor described the [DPPA] bill in the Senate as ‘striking a critical balance between the legitimate governmental and business needs for this information, and the fundamental right of our people to privacy and safety.’” (quoting 139 Cong. Rec. 29468 (1993) (statement of Sen. Boxer))); *Nelson*, 2013 WL 5888235, at *2 (“The [DPPA] does not prescribe methods for collecting, handling, or storing personal information; it merely prohibits persons from obtaining, using or disclosing such information for any purpose not approved under the statute.”); *accord Cook*, 663 F.3d at 996 (“Bulk obtainment of driver information for a permissible purpose does not violate the DPPA.”).

In any event, this Court need not consider the precise contours of what constitutes knowingly obtaining, disclosing, or using private data because Plaintiff has not alleged

that any disclosure by the Commissioners was knowingly for a purpose not permitted under the DPPA. “Under a plain reading of 18 U.S.C. § 2724(a), to be liable a defendant must obtain, disclose, or use personal information, *knowing that it is for a purpose other than one of the permissible purposes.*” *Kiminski*, 2013 WL 6872425, at *6 (emphasis added). In other words, “the person who obtains, discloses, or uses the information must do so *for* an impermissible purpose.” *Id.*; *accord Mallak*, 2014 WL 1285807, at *8 (“[T]he Court agrees with Defendants and other courts in this district that to state a claim under the DPPA, a plaintiff must allege that the information was obtained for a purpose not permitted.”). Such a reading is also consistent the DPPA’s legislative history, particularly co-sponsor Senator Barbara Boxer’s statement that “only those people and individuals who willfully violate this chapter are subject to penalties.” 139 Cong. Rec. S15745-01 (daily ed. Nov. 16, 1993) (statement of Sen. Boxer), *available at* 1993 WL 470986.

Plaintiff alleges that “Defendant Commissioners or the employees they supervised knowingly disclosed Loeffler’s private information from her driver’s license for purposes not permitted under the DPPA.” (Compl. ¶ 187.) “While legal conclusions can provide the framework of a complaint, they must be supported by factual allegations.” *Iqbal*, 556 U.S. at 679. Fatally, Plaintiff has alleged no facts that the Commissioners knowingly disclosed her private data for an impermissible purpose under the DPPA. Nothing in the Complaint’s allegations permits the Court to infer an impermissible purpose on behalf of the Commissioners. *See Kost*, No. 13-cv-583 (JNE/TNL) (Mem. & Ord. at 9-10, Dec. 19, 2013, ECF No. 241) (“Plaintiffs bear the burden of providing enough facts in the

complaint to support an inference that each Defendant accessed their information for an impermissible purpose.”). “The need at the pleading stage for allegations plausibly suggesting (not merely consistent with) [liability] reflects the threshold requirement of Rule 8(a)(2) that the ‘plain statement’ possess enough heft to ‘sho[w] that the pleader is entitled to relief.’” *Twombly*, 550 U.S. at 557. Plaintiff must do more than conclusory plead that the Commissioners disclosed her private data to other individuals and those individuals acted with an impermissible purpose. *See Nelson*, 2013 WL 5888235, at *3.

Relying on *Smythe v. City of Onamia*, No. 12-cv-3149 (ADM/LIB), 2013 WL 2443849 (D. Minn. June 5, 2013), Plaintiff asserts that she “need not allege any ‘misuse’ in her complaint[] because the mere act of accessing the information violates the [DPPA].” (Pl.’s Mem. in Opp’n to Commrs. at 27.) Plaintiff directs this Court to the *Smythe* court’s conclusion that the retrieval of private data violates the DPPA unless the person retrieving the data has done so for a permissible purpose. (*Id.*) Plaintiff’s argument, however, does not remove the DPPA’s requirement that there be an allegation of an impermissible purpose. The *Smythe* court stated:

An officer who retrieves motor vehicle records has violated the DPPA *unless* he or she has done so for a permitted purpose, such as for a law enforcement function. In other words, a person may still violate the DPPA if he retrieves motor vehicle records and does not misuse the information; simply retrieving records without a permitted purpose is a violation. By way of illustration, a police officer might retrieve a celebrity’s motor vehicle records out of curiosity or a desire to learn the celebrity’s age. By doing so, the officer has obtained a motor vehicle record under § 2724(a), but has done so without one of the permitted purposes listed in § 2721(b). As a result, this simple act of retrieval, without any further action, would violate the DPPA. *Similarly, here,*

Smythe alleges Matzke retrieved his personal information out of curiosity or for some personal interest in light of their long and contentious history. Even if Matzke did not go on to misuse Smythe's information, these allegations plausibly state a DPPA violation.

2013 WL 2443849, at *6 (second emphasis added). *Smythe* thus contained allegations that the individual who accessed Smythe's private data had an impermissible purpose under the DPPA. Here, the Complaint contains no allegations of any impermissible purpose on the part of the Commissioners and therefore fails to state a claim under the DPPA.

c. Knowledge of Misuse

Finally, the Commissioners take issue with Plaintiff's allegations that they knew about abuse of the database. The Commissioners argue that, "[e]ven assuming that knowledge of misuse of the database would support a private right of action under the DPPA against the Commissioners as opposed to civil penalties imposed on DPS by the U.S. Attorney General, Plaintiff has not sufficiently ple[aded] facts to support her allegations that the Commissioners knew of such misuse." (Commrs.' Mem. in Supp. at 8.) The Court need not, however, consider the sufficiency of any knowledge allegations because, even assuming the Commissioners knew about abuse of the database by others, there are no allegations that the Commissioners' purpose in creating, maintaining, and granting access to the database was to disseminate private data for impermissible purposes under the DPPA or for the purpose of facilitating others' access of private data for impermissible purposes. *See Potocnik*, 2014 WL 1206403, at *5 ("The fact that the Commissioners were aware of widespread misuse of the DVS database does not mean

that their purpose in creating and maintaining the database was to facilitate that misuse.”). Lastly, this type of knew-or-should-have-known allegation sounds very much in negligence, a concept which, as previously discussed, the courts of this District have deemed incompatible with the plain language of the DPPA. *See Gulsvig*, 2014 WL 1285785, at *6; *Potocnik*, 2014 WL 1206403, at *6; *Kiminski*, 2013 WL 6872425, at *9.

Based on the foregoing, the Court recommends that Plaintiff’s DPPA claims against the Commissioners (Count I) be dismissed for failure to state a claim.

2. Section 1983 Claims

“Section 1983 provides a federal cause of action against anyone who, acting pursuant to state authority, violates any rights privileges or immunities secured by the Constitution and laws of the United States.” *Midwest Foster Care & Adoption Ass’n v. Kincade*, 712 F.3d 1190, 1195 (8th Cir. 2013) (quotations omitted); *see also Potocnik*, 2014 WL 1206403, at *12 (“Section 1983 ‘authorizes suits to enforce individual rights under federal statutes as well as the Constitution.’” (quoting *City of Rancho Palos Verdes v. Abrams*, 544 U.S. 113, 119 (2005))). Specifically,

[e]very person who, under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory or the District of Columbia, subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, suit in equity, or other proper proceeding for redress

42 U.S.C. § 1983. “Section 1983 does not itself create any substantive rights, ‘but merely provides a method for vindicating federal rights elsewhere conferred.’” *Kiminski*, 2013

WL 6872425, at *9 (quoting *Albright v. Oliver*, 510 U.S. 266, 271 (1994)); accord *Mallak*, 2014 WL 1285807, at *9 (“Section 1983 is not itself a source of substantive rights, but is the procedural vehicle through which to vindicate federal rights elsewhere conferred.”). Significantly, § 1983 serves “to vindicate only ‘the violation of a federal right, not merely a violation of federal law.’” *Kincade*, 712 F.3d at 1195 (quoting *Blessing v. Freestone*, 520 U.S. 329, 340 (1997)).

Pursuant to § 1983, Plaintiff alleges the Commissioners violated her statutory rights under the DPPA and constitutional right to privacy under the Fourth and Fourteenth Amendments. (Compl. ¶¶ 247-63.) Plaintiff also seeks prospective relief against Commissioner Dohman. (Compl. ¶¶ 264-71.) The Commissioners move to dismiss Plaintiff’s § 1983 claims in their entirety. The Court will consider each claim in turn.

a. DPPA

The Commissioners assert that § 1983 is not available to Plaintiff for any alleged DPPA violation because the DPPA contains remedies inconsistent with the relief available under § 1983 and, therefore, Congress implicitly foreclosed enforcement of the DPPA via § 1983. (Commrs.’ Mem. in Supp. at 14-16.)

Notably, because Plaintiff has failed to state a claim against the Commissioners under the DPPA, any § 1983 claim asserted against the Commissioners based on a violation of the DPPA necessarily fails. As just discussed, § 1983 provides a means for vindicating rights conferred by the Constitution and other federal statutes. *Kiminski*, 2013 WL 6872425, at *9. “Standing alone, § 1983 does not establish any substantive

rights. An underlying constitutional or statutory violation is a predicate to liability under § 1983.” *Bass*, 2014 WL 683969, at *6 (quotations omitted). Because Plaintiff has failed to state a claim that the Commissioners violated the DPPA, dismissal is warranted on Plaintiff’s § 1983 claims based on the DPPA for lack of a statutory violation. *Gulsvig*, 2014 WL 1285785, at *7; *Bass*, 2014 WL 683969, at *6.

Even assuming *arguendo* that Plaintiff had stated a DPPA claim against the Commissioners, Plaintiff’s § 1983 claim against the Commissioners based on the DPPA still fails. “[T]o sustain a § 1983 action, the plaintiff must demonstrate that the federal statute creates an individually enforceable right in the class of beneficiaries to which [s]he belongs.” *Rancho Palos Verdes*, 544 U.S. at 120. This showing creates “‘a rebuttable presumption that the right is enforceable under § 1983.’” *Id.* (quoting *Blessing*, 520 U.S. at 341). “Defendants can rebut this presumption by showing either that Congress explicitly foreclosed a remedy under § 1983 or implicitly did so, ‘by creating a comprehensive enforcement scheme that is incompatible with individual enforcement.’” *Kincade*, 712 F.3d at 1196 (quoting *Blessing*, 520 U.S. at 341).

Plaintiff asserts that the DPPA is a statutory embodiment of the constitutional right to privacy. (*See* Pl.’s Opp’n to Commrs. at 32-34.) This Court, however, need not decide the rights issue today because, even assuming the DPPA creates a federally protected right, this Court concludes that the DPPA’s comprehensive enforcement scheme forecloses a § 1983 remedy. *See, e.g., Rasmusson*, 2014 WL 107067, at *4 (assuming Plaintiff could “demonstrate that the DPPA constitutes a protectable ‘right’”); *Nelson*, 2013 WL 5888235, at *6 (“[a]ssuming without deciding that the DPPA confers an

individual right to privacy”); *Kiminski*, 2013 WL 6872425, at *11 (assuming but not deciding “that the DPPA creates a federally protected right”); *but see Potocnik*, 2014 WL 1206403, at *12 (“The Court does not doubt that the DPPA creates individually enforceable rights or that Potocnik belongs to the class of individuals that the statute is meant to protect.”).

Significantly, each of this District’s courts to have considered the issue of whether an alleged DPPA violation is enforceable via § 1983 have determined that § 1983 is not available to would-be DPPA plaintiffs. As the *Mallak* court observed, “[t]he courts in this district have thus determined that the DPPA ‘does not leave open the door for a § 1983 action.’” 2014 WL 1285807, at *10 (footnotes and citations omitted) (quoting *Kiminski*, 2013 WL 6872425, at *12). Like the parties, this District’s courts recognize that there is a split of authority on this issue; the Eighth Circuit has not yet addressed it; and, in fact, district courts within the Circuit have reached different conclusions. *Nelson*, 2013 WL 5888235, at *7 (“The Court recognizes that there has been a split of authority on this issue, both among circuits and among district courts with the Eighth Circuit.”); *accord Rasmusson*, 2014 WL 107067, at *5-6 (discussing cases); *Kiminski*, 2013 WL 6872425, at *13-14 (same); *compare Arrington v. Richardson*, 660 F. Supp. 2d 1024, 1035 (N.D. Ia. 2009) (“[T]he DPPA’s remedial scheme complements the relief available under § 1983. Congress neither required plaintiffs to comply with any procedures before filing suit nor did it restrict plaintiffs from obtaining any remedies provided under § 1983.” (citation omitted)), *with Roberts v. Source for Public Data*, 606 F. Supp. 2d 1042, 1046 (W.D. Mo. 2008) (“Given this comprehensive remedial scheme, the Court

must presume that Congress intended that the enforcement scheme it created in the DPPA would be the exclusive remedy for violations, precluding resort to § 1983 by Plaintiffs.”); *see also Collier v. Dickinson*, 477 F.3d 1306, 1311 (11th Cir. 2007) (“Rather than conflicting, we find the relief offered by the DPPA and Section 1983 to be complementary. The DPPA did not create ‘so many specific statutory remedies’ for individual enforcement that it is ‘hard to believe that Congress intended to preserve the § 1983 right of action.’” (quoting *Blessing*, 520 U.S. at 347)); *McCready v. White*, 417 F.3d 700, 703-04 (7th Cir. 2005) (“[Plaintiff] can’t use § 1983 to supply the private right of action missing from § 2724(a).”); *Hurst v. State Farm Mut. Auto. Ins. Co.*, No. 10-1001-GMS, 2012 WL 426018, at *11 n.9 (D. Del. Feb. 9, 2012) (“Appellate courts are split on the issue of whether statutory rights created by the DPPA are enforceable both directly and under § 1983.” (citing cases)). But, notwithstanding the available arguments to the contrary, the courts of this District have uniformly held, as urged by the Commissioners here, that the DPPA’s private remedy is more restrictive and, therefore, incompatible with § 1983. *Potocnik*, 2014 WL 1206403, at *12-13; *Rasmusson*, 2014 WL 107067, at *4-6; *Nelson*, 2013 WL 5888235, at *7; *Kiminski*, 2013 WL 6872425, at *11, 12-14; *see also Mallak*, 2014 WL 1285807, at *10 (adopting the reasoning of *Rasmusson* and *Kiminski*); *Bass*, 2014 WL 683969, at *7 (adopting the reasoning of *Kiminski*).

This Court agrees. In doing so, this Court adopts the analysis of *Kiminski*. *See also Kost*, No. 13-cv-583 (JNE/TNL) (Mem. & Ord. at 16). In *Kiminski*, the court concluded that the range of remedies available under the DPPA (civil fines imposed on

states' department of motor vehicles by the Attorney General, criminal penalties, a private right of action, and the availability of equitable relief in connection with such action) provided a comprehensive enforcement scheme. 2013 WL 6872425, at *12; *accord Rasmusson*, 2014 WL 107067, at *4; *see also Mallak*, 2014 WL 1285807, at *10 (“Various courts have held that, irrespective of whether a plaintiff is able to demonstrate that the DPPA confers a federally protected right . . . , Congress intended to create a comprehensive enforcement scheme through the DPPA and to thereby preclude a remedy under § 1983.”).

With respect to the private cause of action provided in § 2724 of the DPPA, the *Kiminski* court emphasized “the Supreme Court’s guidance in *Rancho Palos Verdes* that an explicit private remedy in a statute should be the key consideration of the analysis.” *Kiminski*, 2013 WL 6872425, at *13; *see Rancho Palos Verdes*, 544 U.S. at 121 (“The provision of an express, private means of redress in the statute itself is ordinarily an indication that Congress did not intend to leave open a more expansive remedy under § 1983.”); *see also Kiminski*, 2013 WL 6872425, at *13 (“The express provision for a private cause of action in the DPPA’s remedial scheme carries significant weight in the analysis.” (citing *Rancho Palos Verdes*, 544 U.S. at 121)). The *Kiminski* court went on to point out that, while similar remedies (actual damages, punitive damages, attorneys’ fees, litigation costs, and equitable relief) are available in both DPPA and § 1983 civil actions, the DPPA does not permit a private action against states and their agencies whereas § 1983 “allows for prospective, injunctive relief against a state actor in his or her official capacity.” *Kiminski*, 2013 WL 6872425, at *13. Accordingly, “[a] concurrent § 1983

action would thus allow access to an additional remedy that Congress did not intend.” *Id.*; *accord Potocnik*, 2014 WL 1206403, at *13 (DPPA private remedy more restrictive because “DPPA precludes lawsuits against states and state agencies, no matter what relief is sought by the plaintiff”); *Rasmusson*, 2014 WL 107067, at *4 (DPPA private remedy more restrictive because, “while an individual may seek injunctive relief under § 1983 against a state official acting in his official capacity, the DPPA expressly excludes civil suits against states and state agencies”); *Nelson*, 2013 WL 5888235, at *7 (DPPA private right of action more restrictive because it “provides a private right of action against *individuals* for violations, but not against a state, its agencies, or—by extension—state employees in their official capacities”).

Additionally, the *Rasmusson* and *Potocnik* courts have pointed out another way in which the DPPA’s private remedy is more restrictive than the remedy available under § 1983: a shorter statute of limitations. “DPPA claims are subject to a four-year statute of limitations” whereas § 1983 claims are subject to a six-year statute of limitations. *Rasmusson*, 2014 WL 107067, at *5; *accord Potocnik*, 2014 WL 1206403, at *12. “Allowing a plaintiff to assert DPPA rights via § 1983 would effectively abrogate the four-year statute of limitations that applies to DPPA claims.” *Potocnik*, 2014 WL 1206403, at *12; *see Mallak*, 2014 WL 1285807, at *10 (“Courts in this district have also determined that the DPPA provides a more restrictive private cause of action than that permitted by § 1983, given the available remedies, relevant limitation periods, and potential defendants for claims asserted under each statute.” (footnotes omitted)).

Plaintiff urges this Court to find that the DPPA's "remedial scheme is insufficiently comprehensive to supplant [§] 1983." (Pl.'s Mem. in Opp'n to Commrs. at 41; *see also id.* at 43.) Plaintiff argues that she "is not bringing suit against the state, or any state actors in their official capacities" and, therefore, the fact that § 1983 permits such litigation is "irrelevant for purposes of individual enforcement of the DPPA and [§] 1983." (*Id.* at 42.) But the determination of whether Congress intended to foreclose enforcement of the DPPA via § 1983 is dependent upon the statutory scheme, not the particular defendants a plaintiff has chosen to sue in a particular lawsuit. *See Rancho Palos Verdes*, 544 U.S. at 120-25 (examining language of statute to determine whether Congress intended to foreclose § 1983 enforcement).

Accordingly, the Court recommends that Plaintiff's DPPA claims asserted against the Commissioners via § 1983 (Count IV), including her claim for prospective relief under § 1983 against Commissioner Dohman (Count V), be dismissed for failure to state a claim.

b. Constitutional Privacy Claims

Lastly, the Commissioners move for dismissal of Plaintiff's constitutional privacy claims based on the Fourth and Fourteenth Amendments "because Plaintiff cannot meet the threshold requirement of showing that driver's license information is the type of intimate information protected from disclosure by the constitutional right of privacy." (Commrs.' Mem. in Supp. at 10.) Relying primarily on *Maracich*, Plaintiff contends that she has a constitutional right of privacy in her private data and the body of caselaw decided prior to *Maracich* holding otherwise "failed to acknowledge that more is

contained in a motor vehicle record than one's address, height, weight, and photograph.” (Pl.'s Mem. in Opp'n to Commrs. at 29 (citing cases).) In this regard, Plaintiff contends that health information and Social Security numbers are also contained in Minnesota's driver's license records. (*Id.* at 28-30.)

“The Constitution protects individuals against invasion of their privacy by the government. The protection against public dissemination of information[, however,] is limited and extends only to highly personal matters representing the most intimate aspects of human affairs.” *McCaslin v. Campbell*, 108 F.3d 1382, at *2 (8th Cir. 1997) (per curiam) (quotations omitted).

Not every disclosure of personal information will implicate the constitutional right to privacy, however, and the Supreme Court has cautioned against unwarranted expansion of the right: “[T]he personal rights found in [the] guarantee of personal privacy must be limited to those which are fundamental or implicit within the concept of ordered liberty.”

Cooksey v. Boyer, 289 F.3d 513, 515-16 (8th Cir. 2002) (alteration in original) (quoting *Paul v. Davis*, 424 U.S. 693, 713 (1976) (internal quotation marks omitted)).

“[T]o violate the constitutional right of privacy[, the information disclosed must be either a shocking degradation or an egregious humiliation to further some specific state interest, or a flagrant breach of a pledge of confidentiality which was instrumental in obtaining the personal information.” *Id.* at 516 (quotation omitted); accord *Van Zee v. Hanson*, 630 F.3d 1126, 1128 (8th Cir. 2011) (same). “A constitutional privacy claim ‘depends upon whether the plaintiff had a reasonable expectation of privacy in the information.’” *Bass*, 2014 WL 683969, at *4 (quoting *Van Zee*, 630 F.3d at 1129).

“Courts also ‘examine the nature of the material opened to public view to assess whether the person had a legitimate expectation that the information would remain confidential while in the state’s possession.’” *Mallak*, 2014 WL 1285807, at *11 (quoting *Eagle v. Morgan*, 88 F.3d 620, 625 (8th Cir. 1996)); accord *Cooksey*, 289 F.3d at 516 (same). “According to the Eighth Circuit, these standards set a high bar and many disclosures, regardless of their nature, will not reach the level of a constitutional violation.” *Rasmusson*, 2014 WL 107067, at *6 (quotation omitted); see also *Potocnik*, 2014 WL 1206403, at *14, 16 (noting the Eighth Circuit has set a “demanding” and “extremely high” standard for constitutional privacy claims).

Beginning with Plaintiff’s contention that *Maracich* can be read to subsume the DPPA’s statutorily defined private data within the constitutional right to privacy, two courts in this District have already rejected this argument. In doing so, the *Rasmusson* and *Mallak* courts noted that the issue of “whether an individual has a *constitutional* right to privacy in driver’s license record information” was not before the Supreme Court in *Maracich*. *Mallak*, 2014 WL 1285807, at *11; accord *Rasmusson*, 2014 WL 107067, at *8. “While the Supreme Court recognized the importance of the information available through motor vehicle databases, it did not hold that this information is constitutionally protected; *Maracich* is therefore not controlling here.” *Mallak*, 2014 WL 1285807, at *11; see also *Rasmusson*, 2014 WL 107067, at *8 (“[T]he statements regarding privacy that the Court did make cannot be understood to refer to a constitutional right rather than to a statutory right.”). This Court agrees with the analysis of *Rasmusson* and *Mallak*.

As for the private data that was allegedly accessed, the Court notes Plaintiff's somewhat ambiguous pleading on this point. At times, the Complaint refers to information that could be in the database: "names, dates of birth, driver's license numbers, addresses, driver's license photos, weights, heights, [S]ocial [S]ecurity numbers, various health and disability information, and eye colors of Minnesota drivers." (Compl. ¶ 64; *see also id.* ¶ 124.) But Plaintiff then goes on to allege that the private data *actually accessed* "includ[ed] her home address, color photograph or image, date of birth, eye color, height, weight, and driver identification number." (Comp. ¶ 96.) *Cf. Potocnik*, 2014 WL 1206403, at *13 ("But Potocnik also includes in her complaint an itemized list of the specific information that she alleges was obtained or disclosed about her, and that list conspicuously fails to include her social-security number or any health or disability information.").

With respect to Plaintiff's address, picture, date of birth, eye color, height, weight, and driver's license number, the courts in this District have soundly rejected any legitimate expectation of privacy in this information. *Mallak*, 2014 WL 1285807, at *11 ("No case has yet found that a constitutional right to privacy exists under the Fourth or Fourteenth Amendment for the type of information typically found in driver's licenses and protected by the DPPA (address, color photograph, date of birth, weight, height, and eye color)."); *see also Gulsvig*, 2014 WL 1285785, at *8 ("Courts have repeatedly found that this type of information—that which is typically found in a motor vehicle record—is *not* the kind of intimate or extremely personal information that gives rise to constitutional protection."); *Potocnik*, 2014 WL 1206403, at *16 ("The information about Potocnik in

the DVS database is statutorily defined as private, but it cannot fairly be said to include the ‘most private details’ of her life.”); *Bass*, 2014 WL 683969, at *5 (“[A]ny expectation of privacy Bass had in the information defendants allegedly accessed is not one society recognizes as reasonable.”); *Rasmusson*, 2014 WL 107067, at *8 (“[T]his information does not warrant constitutional protection because an individual does not have a legitimate expectation of privacy in it.”); *Nelson*, 2013 WL 5888235, at *4 (“The information Nelson alleges was disclosed—his name, date of birth, driver’s license number, address, driver’s license status, driver’s license photo, weight, height, and eye color—while personal, is not particularly sensitive.” (quotation omitted)); *Kiminski*, 2013 WL 6872425, at *15 (“The complaint alleges that the information provided includes their address, color photograph, date of birth, weight, height and eye color, and in some instances, their medical and/or disability information. None of that data qualifies as so extremely personal as to trigger constitutional—as opposed to statutory—privacy protection.” (quotation omitted)).

These courts focused on the fact that this information can be found on the face of a driver’s license and, given that driver’s licenses are routinely presented to strangers under a wide variety of circumstances, “there is no reasonable expectation of privacy in such information.” *Mallak*, 2014 WL 1285807, at *11; *accord Bass*, 2014 WL 683969, at *5 (“A driver’s license contains such information precisely for, among other purposes, identifying oneself to others, cashing checks, using credit cards, boarding airplanes or purchasing age-restricted products.”); *Rasmusson*, 2014 WL 107067, at *8 (“With the exception of Plaintiff’s driving record, all of this information is included on the face of a

driver's license, and individuals show their driver's licenses to strangers on a daily basis."); *Nelson*, 2013 WL 5888235, at *4 ("Like the Fourth Circuit, this Court 'seriously doubt[s]' whether an individual has a reasonable expectation of privacy in any information 'routinely shared with strangers.'" (alteration in original) (quoting *Condon v. Reno*, 155 F.3d 453, 465 (4th Cir. 1998), *rev'd on other grounds*, *Reno v. Condon*, 528 U.S. 141 (2000))). This Court agrees.

Further, much of the information can be obtained from public records and is not uniquely available via the database. *Bass*, 2014 WL 683969, at *5; *accord Rasmusson*, 2014 WL 107067, at *8 ("[M]uch of this information can be obtained by looking at an individual or by reviewing public records."); *Nelson*, 2013 WL 5888235, at *5 ("[T]he same type of information is available from numerous other sources' such as public property tax records." (quoting *Condon*, 155 F.3d at 465)).

Additionally, the DPPA itself contemplates numerous scenarios under which such information can be permissibly disclosed. 18 U.S.C. § 2721(b) (listing permissible uses); *see also Potocnik*, 2014 WL 1206403, at *16 ("[T]here are many scenarios under which Potocnik's DVS driver's-license information could have been lawfully obtained by others, including the defendants in this case."); *Bass*, 2014 WL 683969, at *5 ("Congress expressly recognized numerous situations in which the information contained in motor vehicle records may be lawfully accessed.").

For the reasons stated above, this Court concludes that Plaintiff has no reasonable expectation of privacy in her driver's license information, namely, her address, picture, date of birth, eye color, height, weight, and driver's license number.

While Plaintiff alleges that the database can contain medical information, like Potocnik, Plaintiff “does not allege that she provided any health or disability information to DPS in order to obtain a driver’s license, nor does she allege that she has any health condition or disability that would need to be disclosed.” *Potocnik*, 2014 WL 1206403, at *14. Where plaintiffs have alleged only that the database contained the health information of others but did not allege that their own health information was disclosed as the result of any allegedly impermissible access, the courts of this District have found such allegations conclusory and insufficient to state a constitutional privacy claim. *Mallak*, 2014 WL 1285807, at *12; *Potocnik*, 2014 WL 1206403, at *14; *Rasmussen*, 2014 WL 107067, at *8; *Nelson*, 2013 WL 5888235, at *4; *Kiminski*, 2013 WL 6872425, at *15; *see also Gulsvig*, 2014 WL 1285785, at *8 n.5. This Court agrees.

The same can also be said for the Social Security number allegations. Plaintiff has not specifically alleged that her Social Security number was disclosed in connection with any alleged impermissible access, only that Social Security numbers can be part of the private data contained in the database. *See Gulsvig*, 2014 WL 1285785, at *9 (“Plaintiffs admitted in oral argument that they did not allege in the Complaint that any social security numbers were accessed, so the *potential* for social security numbers to fall within the scope of constitutionally protected information does not suffice to state a claim for a constitutional privacy violation.”).

Similarly, two other courts to have considered that Social Security numbers may be part of the information contained in the database have both concluded that the plaintiff failed to state a claim for a violation of her constitutional right to privacy. *Mallak*, 2014

WL 1285807, at *12; *Potocnik*, 2014 WL 1206403, at *14, 16. Recognizing the sensitive nature of Social Security numbers, these courts found that the interest one has in keeping one's Social Security number confidential does not rise to the level of a constitutionally protectable privacy interest under the Eighth Circuit's high standards. *See Mallak*, 2014 WL 1285807, at *12 ("Even so, a privacy interest and a sensitive or highly confidential designation are not the same as having a constitutional right to privacy. The Court concludes that Plaintiff has not stated a claim based on a constitutional right to privacy in this information."); *Potocnik*, 2014 WL 1206403, at *14, 16 (including Social Security number within information allegedly impermissibly disclosed and concluding such information "cannot fairly be said to include the 'most private details' of [plaintiff's] life"). Accordingly, even if Plaintiff's Complaint could be read to allege that her Social Security number was impermissibly disclosed, Plaintiff has not stated a viable claim based on a constitutional right to privacy in this information.

Whether analyzed under the Fourteenth Amendment or the Fourth Amendment (as applied to the states via the Fourteenth Amendment), a constitutional privacy claim requires a reasonable expectation of privacy in the information at issue. *See Van Zee*, 630 F.3d at 1128 (Fourteenth Amendment privacy claim requires assessment of whether person had legitimate expectation of privacy that information would remain confidential); *Rasmusson*, 2014 WL107067, at *7 ("Similar to the Fourteenth Amendment standards, '[a] search occurs under the Fourth Amendment when . . . the government violates a subjective expectation of privacy that society recognizes as reasonable.'" (quoting *Arnzen v. Palmer*, 713 F.3d 369, 372 (8th Cir. 2013) (alternation in original) (internal

quotation marks omitted)); *see also* *Mallak*, 2014 WL 1285807, at *11 n.18 (“Because the Court finds no reasonable expectation of privacy in the type of data at issue in this case, the Court analyzes violations under both Amendments together in this section.”). Because this Court concludes that Plaintiff does not have a reasonable expectation of privacy in her driver’s license information, Plaintiff has failed to state a constitutional privacy claim under either Amendment.⁵ *Mallak*, 2014 WL 1285807, at *12; *Rasmusson*, 2014 WL107067, at *8; *accord* *Bass*, 2014 WL 683969, at *5; *Nelson*, 2013 WL 5888235, at *5; *see* *Potocnik*, 2014 WL 1206403, at *16; *Kiminski*, 2013 WL 6872425, at *15.

Therefore, because Plaintiff has no reasonable expectation of privacy in the information allegedly accessed, this Court recommends that Plaintiff’s constitutional privacy claims against the Commissioners (Count IV) be dismissed.

B. Dakota County

Plaintiff’s allegations against Dakota County encompass three types of defendants: Dakota County itself; Dakota County employees, including law enforcement; and supervisors employed by Dakota County. (*See* Compl. ¶¶ 11, 42, 44-46.) Plaintiff alleges that “[o]fficers employed by, licensed by, or otherwise accessing through Dakota County impermissibly accessed [her p]rivate [d]ata three times.” (*Id.* ¶ 69; *see also id.* ¶ 136.) Plaintiff alleges that such accesses occurred by “view[ing her] Private Data from

⁵ Because the Court finds the lack of a reasonable expectation of privacy to be dispositive of Plaintiff’s constitutional privacy claims, the Court does not consider whether the alleged accesses of her driver’s license information constitute a search under the Fourth Amendment. *Cf. Potocnik*, 2014 WL 1206403, at *13 (“No court has ever held that accessing a driver’s-license database constitutes a search or seizure within the meaning of the Fourth Amendment.”); *Bass*, 2014 WL 683969, at *6 (no search occurs under the Fourth Amendment if there was no reasonable expectation of privacy).

her State-issued driver's license including her home address, color photograph or image, date of birth, eye color, height, weight and driver identification number.” (*Id.* ¶ 96.) Plaintiff alleges that these accesses occurred by entering her name into the database, “not her license plate number, to look up her private, personal information.” (*Id.* ¶ 137.) Plaintiff alleges that these “accesses were impermissible, meaning that the Defendants had no law-enforcement reason for accessing the information. Defendants accessed the information for personal reasons completely unrelated to their position as law-enforcement officers.” (*Id.* ¶ 95; *see also id.* ¶¶ 158, 188-90.) Plaintiff further alleges that Dakota County supervisors “should have monitored, prevented and stopped the unauthorized access [of Plaintiff's] information” by Dakota County employees. (*Id.* ¶ 139.) Plaintiff also alleges that Dakota County and its supervisors “permitted, condoned, or acquiesced in this illegal access to Plaintiff's private information, and knew or should have known that it was occurring.” (*Id.* ¶ 145; *see also id.* ¶¶ 144, 192.)

1. Statutes of Limitation

The Court begins with Dakota County's argument that all of Plaintiff's claims are *likely* barred by statutes of limitation. (*See* Dakota Cnty.'s Mem. in Supp. at 23-26, ECF No. 35.) “A court may dismiss a claim under Rule 12(b)(6) as barred by the statute of limitations if the complaint itself establishes that the claim is time-barred.” *Illig v. Union Elec. Co.*, 652 F.3d 971, 976 (8th Cir. 2011). Dakota County acknowledges, however, that Plaintiff has “fail[ed] to include information regarding the date and time of the alleged look-ups by Dakota County.” (Dakota Cnty.'s Mem. in Supp. at 23.) Indeed, attached to Plaintiff's Complaint as Exhibit A is a copy of an audit prepared by DPS

showing accesses of Plaintiff's information. (Compl. ¶ 3, Ex. A, ECF. No. 1-1.) While Exhibit A includes the day of the alleged access in the "AccessDay" column, the "AccessDate" column is curiously blank. (*Id.* Ex. A.)

Plaintiff responds that she "mistakenly failed to specifically articulate the date and time of each alleged violation." (Pl.'s Mem. in Opp'n to Dakota Cnty. at 43, ECF No. 63.) Plaintiff goes on to state that she "incorporated by reference her entire DPS audit, which was incompletely attached to her Complaint. . . . The full audit, intended to be filed with the Complaint, is referenced in the Complaint, and attached to the Declaration of Kenneth H. Fukuda [filed along with Plaintiff's opposition to Dakota County's motion]." (*Id.* at 43-44; *see also* Ex. C to Decl. of Kenneth H. Fukuda, ECF No. 64-2.) Plaintiff argues that "[t]he audit is 'necessarily embraced by the complaint,' and not a document 'outside the pleading.'" (*Id.* at 44 (quoting *Enervations, Inc. v. Minn. Mining & Mfg. Co.*, 380 F.3d 1066, 1069 (8th Cir. 2004)).)

The question, therefore, is whether the Court will consider the "complete" audit contained in Exhibit C of the Fukuda Declaration. When considering a motion to dismiss under Fed. R. Civ. P. 12(b)(6), "the court generally must ignore materials outside the pleadings." *Porous Media Corp. v. Pall Corp.*, 186 F.3d 1077, 1079 (8th Cir. 1999). The court may, however, "consider some materials that are part of the public record or do not contradict the complaint as well as materials that are necessarily embraced by the pleadings." *Id.* (quotations and citation omitted); *see also Illig*, 652 F.3d at 976 ("In addressing a motion to dismiss, the court may consider the pleadings themselves, materials embraced by the pleadings, exhibits attached to the pleadings, and matters of

public record.” (quotation omitted)). “[D]ocuments ‘necessarily embraced by the complaint’ are not matters outside the pleading.” *Enervations*, 380 F.3d at 1069. “[T]he court has complete discretion to determine whether or not to accept any material beyond the pleadings that is offered in conjunction with a Rule 12(b)(6) motion.” *Stahl v. United States Dep’t of Agric.*, 327 F.3d 697, 701 (8th Cir. 2003) (quotation omitted).

The Court exercises its discretion not to consider the additional material Plaintiff submitted in connection with her opposition to Dakota County’s motion, including but not limited to Exhibit C. Notably, Exhibit C is *not* just a more complete version of Exhibit A. According to Exhibit C, the three alleged accesses by Dakota County occurred on *different* days than the accesses listed in Exhibit A. Exhibit A shows one alleged access occurring on a Wednesday and two accesses occurring on a Monday. (Compl. Ex. A.) Exhibit C shows two accesses on a Friday and one on a Tuesday. (Ex. C to Fukuda Decl.) Plaintiff offers no explanation for the discrepancy.⁶ Significantly, because the Court concludes that Plaintiff has failed to state a claim against Dakota County for the reasons discussed below, the actual date of the alleged accesses is irrelevant.

Moreover, the statutes-of-limitation issues are more complicated⁷ in this case based on Plaintiff’s allegations that she initially contacted DPS in 2011 to determine whether her private data had been accessed and was told by DPS “that such information

⁶ In the memorandum supporting their motion to dismiss, the Cities also point out the discrepancy between the days of the accesses in Exhibit A and information that Plaintiff provided directly to the Cities themselves regarding the access dates. (Cities’ Mem. in Supp. at 4, ECF No. 56.) Plaintiff does not address the discrepancy in her responsive memorandum to the Cities either.

⁷ Such complexity is evidenced in part by the fact that Plaintiff devotes over 30% of her memorandum in opposition to statutes-of-limitation issues. (See Pl.’s Mem. in Opp’n to Dakota Cnty. at 17-28, 39-42.)

regarding the [database] could not be provided to [her] unless she had a specific reason for requesting that information.” (Compl. ¶ 57.) Plaintiff subsequently contacted DPS again approximately two years later and was provided with the audit that led to the instant lawsuit. (*Id.* ¶¶ 60-62.) Because the Court need not determine precisely when the alleged accesses occurred in order to resolve the matters raised in Dakota County’s motion to dismiss, the Court declines to address any arguments pertaining to statutes of limitation.

2. DPPA

Dakota County first asserts that, “[a]lthough Plaintiff generally alleges that she brings this action under ‘18 U.S.C. § 2721 *et seq.*,’ she fails to allege specifically what section of the DPPA Dakota County has allegedly violated.” (Dakota Cnty.’s Mem. in Supp. at 8.) Dakota County argues that “Plaintiff rests her allegations on the language of [§] 2721(a),” but “[§] 2721 . . . specifically applies to a ‘State department of motor vehicles, and any officer, employee, or contractor’ of the State department, and does not apply to municipalities such as Dakota County.” (*Id.* (citation omitted).) Plaintiff responds that “[t]his Complaint was brought against [Dakota County] under § 2724(a)” and § 2724(a) is included within the statutory provisions cited. (Pl.’s Mem. in Opp’n to Dakota Cnty. at 7.)

Dakota County’s argument is rather perplexing. Section 2724 of the DPPA supplies a civil cause of action for individuals whose information has been impermissibly accessed “for a purpose not permitted *under this chapter.*” 18 U.S.C. § 2724(a) (emphasis added). Section 2724 does not list permissible or impermissible uses; such

uses are set forth in §§ 2721 and 2722. *See id.* §§ 2721(b) (listing permissible uses); 2722 (proscribing additional unlawful acts). Dakota County has cited no authority affirmatively establishing separate causes of action under the various sections of the DPPA and the plain language of § 2724 indicates otherwise.⁸

Dakota County's primary argument is that Plaintiff must allege more than simply the viewing of her private data. (*See* Dakota Cnty.'s Mem. in Supp. at 9-15.) Dakota County argues that, in order "to obtain" private data within the meaning of the DPPA, a defendant must do more than just view the plaintiff's private data. (*Id.* at 9.) According to Dakota County, Plaintiff has "fail[ed] to allege any facts as to who specifically viewed her information, what the person did with the information once they viewed it, if the person in fact disclosed or used the information after they viewed it, or for what purpose the person disclosed or used the information they viewed." (*Id.* at 14.)

⁸ Dakota County cites *Foos v. Verizon Business Network Services, Inc.*, Civ. No. 10-cv-3040-PA, 2010 WL 3824073 (D. Or. Sept. 22, 2010), and *Hurst* in support of its separate-causes-of-action argument. The entirety of the court's discussion in *Foos* is as follows:

In the complaint, plaintiffs allege the searches were "in violation of the provisions of 18 U.S.C. § 2722(b)" (Compl., ¶ 26.) Plaintiffs now concede, however, that they bring no claim under § 2722. (Pls.' Mem. In Resp., 28.) (Any DPPA claim "is solely based upon the provisions of Section 2724(a)") Therefore, I deny as moot defendants' motions to dismiss plaintiffs' § 2722 claim.

2010 WL 3824073, at *7. *Hurst* involved information that, although substantively of the type encompassed by the DPPA, had not been obtained through a state department of motor vehicles. 2012 WL 426018, at *3, 10. Rather, the information was obtained in connection with an auto insurance policy and the alleged disclosure was made by the insurer in litigation over the policy. *Id.* at *3. *Hurst* subsequently sued the insurer for violations of the DPPA. *Id.* at *2. In concluding that *Hurst* had failed to state a claim under the DPPA, the court noted that "it is far from clear that the Affidavit in question is a motor vehicle record" and "[e]ven if the Affidavit is a motor vehicle record, the complaint does not allege that any defendants performed a search with any state DMV or that they caused a DMV search to be made by a third party to obtain *Hurst*'s 'personal information.'" *Id.* at *10. Here, Plaintiff alleges that the impermissible accesses occurred by means of the database maintained by DPS. Neither of these cases can be read to establish separate causes of action under various sections of the DPPA outside of § 2724.

In addition, Dakota County asserts that Plaintiff is “attempt[ing] to shift the burden to Dakota County of detailing a proper purpose for the access of the data, arguing that Plaintiff lacks the ability to ascertain the specific reason for Dakota County’s access without discovery.” (Dakota County’s Reply at 4-5, ECF No. 69.) Dakota County asserts that, “[b]ecause [Plaintiff’s] complaint does not allege any facts to support a plausible inference that Dakota County’s access of her data fell outside of [permissible use by a government agency], and any other, permissible use, her complaint should be dismissed for failure to state a claim.” (*Id.*)

Relying again on *Smythe*, Plaintiff responds that merely accessing her private data is sufficient to state a claim under the DPPA. (Pl.’s Mem. in Opp’n to Dakota Cnty. at 11; *see also id.* at 13-14.) Plaintiff contends that “as long as [she] has alleged a retrieval of records and alleged the retrieval was made without a permitted purpose, this is enough to state a viable claim under the DPPA.” (*Id.* at 12.)

The Court need not resolve whether the viewing of Plaintiff’s private data constitutes obtaining such information for purposes of the DPPA because, as previously discussed with respect to the Commissioners, Plaintiff has not alleged that any access by Dakota County was knowingly for a purpose not permitted by the DPPA. The extent of Plaintiff’s factual allegations is that her private data was accessed for reasons other than law enforcement. Notably, with the exception of Defendant Female Officer, Plaintiff makes the same allegations with respect to all defendant cities and counties and their personnel.

“Under the DPPA, the plaintiff has the burden of pleading that a defendant accessed a motor vehicle record with an impermissible purpose.” *Bass*, 2014 WL 683969, at *3; *accord Mitchell v. Aitkin Cnty.*, No. 13-cv-2167 (JNE/FLN), 2014 WL 835129, at *7 (D. Minn. Mar. 4, 2014) (“burden of establishing an impermissible purpose lies with the plaintiff”). Plaintiff globally alleges that the counties, cities, and their personnel accessed her private data for “personal reasons” unrelated to law enforcement functions or any of the DPPA’s other permissible uses. (Compl. ¶¶ 95, 188-89.) Fundamentally, “[Plaintiff’s] DPPA claims . . . relate to particular retrievals of her personal information by individual officers. Her claims against them need to be assessed individually and separately. [Plaintiff] therefore needs to allege facts reflecting the impropriety of the data retrieval by each individual officer to raise her claim against the officer above a speculative level.” *Mitchell*, 2014 WL 835129, at *6 (citation omitted); *see also Kost v. Hunt*, No. 13-cv-583 (JNE/TNL), ___ F. Supp. 2d ___, 2013 WL 6048921, at *11 (D. Minn. Nov. 15, 2013) (*Kost II*) (“[A]lthough Plaintiff have sued Defendants in a single action, Plaintiffs’ claims against each Moving Defendant must be evaluated independently.”).

Plaintiff essentially is asking the Court to speculate as to the purposes of Dakota County and its personnel in accessing her private data. Much like the facts alleged in *Mitchell*, Plaintiff’s allegations “do not reflect an outward manifestation of the alleged impermissible purpose” of any Dakota County defendant. *Id.* Beyond the general allegations echoing through this District’s recent DPPA cases (accesses occurred by entering plaintiff’s name, accesses made by multiple government agencies, no criminal

activity by plaintiff, no law enforcement purpose for access, and citation to report addressing widespread abuse of database by law enforcement), Plaintiff cites her ex-husband's employment in law enforcement and his affair with another law enforcement officer to support her contention that Dakota County impermissibly accessed her private data. (*See* Pl.'s Mem. in Opp'n to Dakota Cnty. at 8-10.) But while Plaintiff contends that it is "particularly pertinent" that she "was known to other police officers and had a contentious relationship with certain members of law enforcement," there are no facts alleging that such individuals were employed by Dakota County. *Cf. Smythe*, 2013 WL 2443849, at *6 (noting "long and contentious history" between plaintiff and defendant law enforcement officer); *see Mitchell*, 2014 WL 835129, at *8 ("cases where claims of impermissible purpose have risen above the speculative level . . . generally included some indication of a connection or interaction between an identifiable law enforcement officer and the plaintiff, from which the asserted impropriety of the officer's retrieval of the plaintiff's data can be plausibly inferred"); *see also Ray v. Anoka County*, No. 14-cv-539 (PAM/TNL), ___ F. Supp. 2d ___, 2014 WL 2511087, at *5 (D. Minn. June 4, 2014) (where plaintiff did not plead facts linking those individuals whom she suspected of accessing her driver's license information to defendant jurisdictions, court had no basis to infer that law enforcement officers in defendant jurisdictions had a personal connection to or interest in plaintiff). As a result, "accepting [Plaintiff's] position requires drawing inferences about what went on in a particular officer's mind in connection with a particular lookup, based on assumptions about law enforcement officers generally and contentions about [Plaintiff] personally." *Mitchell*, 2014 WL 835129, at *6.

Plaintiff has failed to allege facts that would permit this Court to reasonably infer that Dakota County and its personnel accessed her private data for an impermissible purpose. Plaintiff must allege facts showing that she is entitled to relief, not merely facts consistent with liability. *See Twombly*, 550 U.S. at 557. As the *Bass* court stated, “the legislative history of the DPPA indicates that Congress intended to preserve broad discretion for government entities and agents in accessing motor vehicle records. As a result, the court will not infer from bare, conclusory allegations that defendants’ purposes were improper.” *Bass*, 2014 WL 683969, at *4 (citation omitted); *see also Smythe*, 2013 WL 2443849, at *5 (“With the exception of misuse, the DPPA’s legislative history indicates a desire to preserve broad discretion for law enforcement agents to retrieve information in the course of their duties.”).

Moreover, to hold otherwise,

would be to allow any person whose data has been retrieved by a governmental entity to proceed with a DPPA action, at least until the defendant provides the reason for accessing the plaintiff’s data. In other words, the civil action provision of the DPPA would need to be read as creating a right to learn of the reason for any personal data retrieval by a governmental agency defendant. But the plain language of the statute does not create that right. Neither does the statute imply it, because the burden of establishing an impermissible purpose lies with the plaintiff. . . . Additionally, . . . finding that the DPPA creates a broad and automatic entitlement to discovery of the reasons a law enforcement officer retrieves an individual’s personal information would contravene the acknowledged discretion that has been recognized for law enforcement activities.

Mitchell, 2014 WL 835129, at *7 (citations omitted); *see also Kost v. Hunt*, No. 13-cv-583 (JNE/TNL), 2013 WL 5566045, at *5 (D. Minn. Oct. 8, 2013) (*Kost I*) (“Allowing

Plaintiffs to conduct discovery based on their complaint—which fails to identify any facts supporting their contention that someone at a governmental entity retrieved their personal information for an impermissible purpose—would create burdens on law enforcement that there is no indication Congress intended to create in enacting the DPPA.”).

Based on the foregoing, the Court concludes that Plaintiff has failed to state a DPPA claim against Dakota County and its personnel and, therefore, recommends that Dakota County’s motion be granted with respect to Count I.

3. Section 1983 Claims

Dakota County also moves for dismissal of Plaintiff’s § 1983 claims based on violations of the DPPA and her Fourth and Fourteenth Amendment rights. In doing so, Dakota County raises the same arguments as the Commissioners, namely that (1) the DPPA contains a comprehensive remedial scheme, precluding relief under § 1983, and (2) Plaintiff does not have a constitutional privacy interest in the information allegedly accessed.

a. DPPA

For the same reasons stated above with respect to the Commissioners, the Court concludes that Plaintiff has failed to state a § 1983 claim based on violations of the DPPA against Dakota County and its personnel.

b. Constitutional Privacy Claims

With respect to Plaintiff’s § 1983 constitutional privacy claims, the Court reiterates that Plaintiff does not have a legitimate expectation of privacy in the information allegedly accessed. Again, Plaintiff does not allege that Dakota County

personnel accessed her Social Security number or any health information, or that Plaintiff even provided health information to DPS. The Court also notes that the entirety of Plaintiff's discussion on this point is to "incorporate[] by reference the Constitutional arguments set forth [in her response to the Commissioner's motion]." (Pl.'s Mem. in Opp'n to Dakota Cnty. at 28.) Therefore, for the reasons stated above, the Court recommends that Dakota County's motion be granted as to Plaintiff's § 1983 claims based on violations of the Fourth and Fourteenth Amendments.

c. *Monell* Claims

There is one additional aspect of Plaintiff's § 1983 constitutional claims that needs to be addressed. Albeit raised in the context of qualified immunity,⁹ Dakota County also argues that Plaintiff has failed to state a *Monell* claim because the Complaint contains insufficient allegations establishing "there was an unconstitutional custom, policy, or practice of viewing driver's license information in Dakota County." (Dakota Cnty.'s Mem. in Supp. at 21; *see also* Dakota Cnty.'s Reply at 10; Compl. ¶¶ 144-52, 197.)

"In *Monell v. Department of Social Services*, the Supreme Court held that a municipality can be liable under § 1983 if an 'action pursuant to official municipal policy of some nature caused a constitutional tort.'" *Veatch v. Bartels Lutheran Home*, 627 F.3d 1254, 1257 (8th Cir. 2010) (citation omitted) (quoting 436 U.S. 658, 691 (1978)). Accordingly, "[a § 1983] claim against a county is sustainable only where a constitutional violation has been committed pursuant to an official custom, policy, or practice." *Luckert*

⁹ Having concluded that there were no underlying constitutional violations, the Court declines to address whether Dakota County and its personnel are entitled to qualified immunity. *See Brockinton v. City of Sherwood*, 503 F.3d 667, 672 (8th Cir. 2007) ("If the facts do not show a [constitutional] violation, we need not proceed further with the qualified immunity analysis.").

v. Dodge Cnty., 684 F.3d 808, 820 (8th Cir. 2012) (quotation omitted). “[t]he Eighth Circuit has consistently recognized a general rule that, in order for municipal liability to attach, individual liability must first be found on an underlying substantive claim.” *Brockinton*, 503 F.3d at 674 (quotation omitted); *see also Bass*, 2014 WL 683969, at *6 (“A municipality, however, may not be held liable for its officers’ actions unless the officers are found liable on the underlying substantive claim.” (quotation omitted)).

Because this Court concludes that Plaintiff has failed to state a claim under § 1983 for violation of her constitutional rights, it necessarily follows that Plaintiff has failed to state a *Monell* claim against Dakota County. *Brockinton*, 503 F.3d at 674; *see also Ray*, 2014 WL 2511087, at *6; *Mallak*, 2014 WL 1285807, at *13 (“Because Plaintiff has not established an underlying violation of any constitutional right, any *Monell* claim against the City and County Defendants must be dismissed.” (citation omitted)); *Bass*, 2014 WL 683969, at *6 (“As already explained, all constitutional claims against the individual defendants fail. As a result, dismissal of the municipal liability claims against the City Defendants is warranted.”).

In sum, the Court concludes that Plaintiff has failed to state a § 1983 claim against Dakota County and its personnel, whether based on the DPPA or constitutional privacy rights, and recommends that Dakota County’s motion be granted with respect to Counts II and III.

4. Invasion of Privacy

Dakota County also moves for dismissal of Plaintiff’s common law, intrusion-upon-seclusion privacy claim (Count VI). Plaintiff alleges that “[b]y improperly

obtaining [her] private personal information for impermissible reasons, Defendants intentionally intruded upon the solitude or seclusion of [her] private affairs and concerns” and that such an “intrusion would be highly offensive to a reasonable person.” (Compl. ¶¶ 273-74.) Dakota County asserts that the alleged intrusion is not one that would be highly offensive to a reasonable person because driver’s license data is routinely presented to others in a wide variety of circumstances and may otherwise be publicly available through other sources. (Dakota Cnty.’s Mem. in Supp. at 22-23.) Additionally, Dakota County argues that “Plaintiff does not allege that by viewing her information, that information was communicated to the public at large or to so many people that the matter must be regarded as substantially certain to become one of public knowledge.” (*Id.* at 23.)

Plaintiff counters that the offensiveness of the intrusion is a question of fact for the jury. (Pl.’s Mem. in Opp’n to Dakota Cnty. at 38, 39.) Plaintiff recognizes, however, that offensiveness becomes a question of law if reasonable people can only draw one conclusion from the evidence. (*Id.* at 38.) *See, e.g., R.S. ex rel. S.S. v. Minnewaska Area Sch. Dist. No. 2149*, No. 12-cv-588 (MJD/LIB), 894 F. Supp. 2d 1128, 1147 (D. Minn. 2012) (“Application of this ‘reasonable person standard’ is typically a question of fact, but it can become a question of law ‘if reasonable persons can draw only one conclusion from the evidence.’” (quoting *Swarthout v. Mut. Serv. Life Ins. Co.*, 632 N.W.2d 741, 745 (Minn. App. 2001))). Plaintiff contends:

Whereas one person intruding in one instance upon [her] privacy by accessing her information on the [database] might not be “highly offensive,” that is not the scenario here. Under

the facts in this case, dozens of law enforcement officials impermissibly obtained [her] personal information more than 130 times. The sheer numbers of the accesses would lead a reasonable person to find the intrusion “highly offensive.”

(Pl.’s Mem. in Opp’n to Dakota Cnty. at 39.)

“Intrusion upon seclusion occurs when one intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns if the intrusion would be highly offensive to a reasonable person.” *Lake v. Wal-Mart Stores, Inc.*, 582 N.W.2d 231, 233 (Minn. 1998) (quotation omitted). “The tort has three elements: (a) an intrusion; (b) that is highly offensive; and (c) into some matter in which a person has a legitimate expectation of privacy.” *Swarthout*, 632 N.W.2d at 744. “There is no liability unless the interference with the plaintiff’s seclusion is a substantial one, of a kind that would be highly offensive to the ordinary reasonable person, as the result of conduct to which the reasonable person would strongly object.” *Id.* at 745 (quotation omitted).

“Minnesota courts have indicated that plaintiffs must meet a high threshold of offensiveness and expectation of privacy to have a viable claim for intrusion upon seclusion.” *Rasmusson*, 2014 WL 107067, at *10. “The ‘highly offensive’ nature of the intrusion is generally a fact question for the jury, but a court must determine whether a certain threshold of ‘offensiveness’ exists for the plaintiff to have a cause of action for intrusion.” *Freeland v. Fin. Recovery Servs., Inc.*, No. 10-cv-3029 (PAM/TNL), 790 F. Supp. 2d 991, 995 (D. Minn. 2011); accord *Bass*, 2014 WL 683969, at *7 (“Invasion of privacy claims involve a preliminary determination of offensiveness which must be made

by the court in discerning the existence of a cause of action.” (quotation omitted)); *see also Swarthout*, 632 N.W.2d at 745 (“[Q]uestions about the reasonable person standard are ordinary questions of fact, but they become questions of law if reasonable persons can draw only one conclusion from the evidence.” (quotation omitted)).

Initially, the Court observes that Plaintiff’s contention that “dozens of law enforcement officials impermissibly obtained [her] personal information more than 130 times,” (Pl.’s Mem. in Opp’n to Dakota Cnty. at 39), is somewhat disingenuous in the context of Dakota County’s motion to dismiss. Dakota County and its personnel are only alleged to have accessed Plaintiff’s information a total of three times. While the Court is to consider the number and frequency of the alleged intrusions in evaluating their offensiveness, *Freeland*, 790 F. Supp. 2d at 995, Plaintiff has given the Court no basis to infer that *all* of the alleged impermissible accesses at issue in this litigation should be attributed to Dakota County. *See Kost II*, 2013 WL 6048921, at *12 (“Although Plaintiffs assert similar [DPPA] claims against the Moving Defendants, the claims stand alone, as no concert of action has been alleged.”).

In any event, much like Plaintiff’s constitutional privacy claims, the courts in this District that have considered the alleged intrusion—the accessing of an individual’s private data via the database—have all concluded that it is not of the type that would be highly offensive to a reasonable person. *Mallak*, 2014 WL 1285807, at *14 (“Here, the Court finds that ‘reasonable persons can draw only one conclusion from the evidence’—that the access of information as alleged by Plaintiff cannot rise to the level of offensiveness required to state a claim for invasion of privacy.”); *Potocnik*, 2014 WL

1206403, at *17 (“And as for the remaining information in the DVS database, the Court agrees with other courts in this district that the act of obtaining or disclosing such information would not be highly offensive to an ordinary reasonable person.” (footnote omitted)); *Bass*, 2014 WL 683969, at *7 (“No reasonable person could find that the alleged access of such information meets the ‘highly offensive’ threshold.”); *Nelson*, 2013 WL 5888235, at *8 (“While the unauthorized access of another’s motor-vehicle records is no doubt an intrusion into another’s private affairs, no reasonable person could consider the intrusion in this case highly offensive.”); *accord Rasmusson*, 2014 WL 107067, at *10 (“Plaintiff’s allegations in this case fail to meet the high threshold for offensiveness and expectation of privacy established by Minnesota law.”).

These courts have again focused on the fact that the information contained in the database is present on individual driver’s licenses, which are routinely displayed thereby reducing an expectation of privacy in the information, and is available from a variety of other sources.¹⁰ *Mallak*, 2014 WL 1285807, at *14; *Potocnik*, 2014 WL 1206403, at *17; *Bass*, 2014 WL 683969, at *7; *Rasmusson*, 2014 WL 107067, at *10; *Nelson*, 2013 WL 5888235, at *8. This Court agrees with the reasoning of *Mallak*, *Potocnik*, *Bass*, *Rasmusson*, and *Nelson*, and concludes that Plaintiff has failed to state a claim for intrusion upon seclusion against Dakota County because the alleged intrusions would not be highly offensive to a reasonable person. Therefore, the Court recommends that Dakota County’s motion to dismiss be granted with respect to Count VI.

¹⁰ The Court again notes that there are no allegations that Plaintiff’s medical information or Social Security number was accessed.

C. Counties

Like the allegations against Dakota County, Plaintiff's allegations against the Counties encompass three types of defendants: the Counties themselves, the Counties' employees, and supervisors employed by the Counties. (Compl. ¶¶ 12-15, 17-18, 42, 44-46.) And, as this Court earlier observed, Plaintiff makes the same allegations with respect to all of the Counties and their personnel. *See supra* III(B)(2). Plaintiff alleges that the impermissible accesses occurred by "view[ing her] Private Data from her State-issued driver's license including her home address, color photograph or image, date of birth, eye color, height, weight and driver identification number." (Compl. ¶ 96.) Plaintiff alleges that these accesses occurred by entering her name into the database, "not her license plate number, to look up her private, personal information." (*Id.* ¶ 137.) Plaintiff alleges that these "accesses were impermissible, meaning that the Defendants had no law-enforcement reason for accessing the information. Defendants accessed the information for personal reasons completely unrelated to their position as law-enforcement officers." (*Id.* ¶ 95; *see also id.* ¶¶ 158, 188-90.) Plaintiff further alleges that the Counties' supervisors "should have monitored, prevented and stopped the unauthorized access [of Plaintiff's] information" by the Counties' employees. (*Id.* ¶ 139.) Plaintiff also alleges that the Counties and their supervisors "permitted, condoned, or acquiesced in this illegal access to Plaintiff's private information, and knew or should have known that it was occurring." (*Id.* ¶ 145; *see also id.* ¶¶ 144, 192.) With respect to the Counties, there are 19 allegedly impermissible accesses at issue: Isanti

County (2), Mille Lacs County (2), Renville County (2), Rice County (2), Wright County (3), and Yellow Medicine County (8). (*Id.* ¶¶ 76, 80, 85, 86, 93, 94; *see also id.* ¶ 136.)

1. DPPA

Similar to Dakota County, the Counties assert that it is not sufficient for Plaintiff to allege only that her information was viewed. The Counties argue that “the DPPA’s plain language establishes that obtaining personal information is not a violation of the statute unless it is thereafter *employed* in some manner” and “a plaintiff cannot state a civil cause of action under the DPPA unless she can sufficiently allege that her personal information was obtained from a motor vehicle record and was also impermissibly used.” (Cnties.’ Mem. in Supp. at 4, 8-9, ECF No. 42.)

In addition to Plaintiff’s failure to allege any subsequent misuse of her private data, the Counties go on to argue that Plaintiff’s Complaint lacks “facts supporting the allegation that [her] personal information was obtained for a ‘purpose not permitted under’ the DPPA.” (*Id.* at 9.) The Counties argue that there are no facts from which the Court can plausibly infer that the accesses by the Counties and their personnel were for an impermissible purpose, and that Plaintiff is essentially trying to shift the burden to the Counties to justify their accesses of Plaintiff’s information. (*Id.* at 10; *see also* Cnties.’ Reply at 1-3, ECF No. 74.) The Counties note the “chilling effect” such a construction would have on law enforcement:

Allowing Plaintiff’s claims to go forward as pled would essentially subject all law enforcement personnel to automatic and significant liability and criminal penalties unless they can specifically recall the reason behind each access of an individual’s information, even if Plaintiff cannot allege

specific facts supporting the allegation that the officer's actions were improper.

(*Id.* at 12.)

To support their argument regarding the conclusory nature of Plaintiff's allegations, the Counties rely largely on the *Kost* case from this District and *Foos*. In particular, the Counties cite to the following excerpt from *Foos*:

Defendants argue plaintiffs fail to plead defendants obtained the information for a purpose not permitted. Plaintiffs do allege defendants obtained and used "Plaintiff's personal information for a purpose not permitted under the DPPA" (Compl., ¶ 27.) At the motion to dismiss stage, however, "formulaic recitation of the elements of a cause of action will not do." *Twombly*, 550 U.S. at 555. "While legal conclusions can provide the framework of a complaint, they must be supported by factual allegations." *Iqbal*, 129 S. Ct. at 1950. Plaintiffs also allege defendants used the information for "unknown reasons." (Compl., ¶ 25.) Merely pleading an "unknown reason" clearly is not a specific factual allegation allowing the court to reasonably infer defend[ants] here used the information for an impermissible purpose.

2010 WL 3824073, at *5.

The Counties contend that

[a]side from formulaic recitations of the elements that [the Counties] illegally viewed her private, personal, and confidential driver's license information without a legitimate or permissible law-enforcement or any other lawful purpose, Plaintiff makes no factual allegations regarding how her information was used by [the Counties] after it was viewed or the "impermissible purpose" for which her information was viewed by the [the Counties].

(Cnties.' Mem. in Supp. at 13.) In this vein, the Counties assert that the accesses of Plaintiff's information need to be evaluated independently and that the Complaint

contains no facts showing that any of the contentious relationships Plaintiff allegedly had with certain law enforcement officers included the Counties' law enforcement officers. (Cnties.' Reply at 2, 3.)

The Counties' second argument—Plaintiff's failure to allege facts from which the Court can plausibly infer that the accesses by the Counties and their personnel were for an impermissible purpose—reaches the nub of the issue. Accordingly, while Plaintiff robustly responds on the finer points of obtainment and use under the DPPA, the Court directly turns to the sufficiency of Plaintiff's allegations that such accesses were knowingly for a purpose not permitted by the DPPA.

Just as with Dakota County, the Complaint must allege facts regarding each of the Counties that would allow the Court to reasonably infer that a particular County, or Counties, knowingly accessed Plaintiff's private data for an impermissible purpose. *Kost II*, 2013 WL 6048921, at *11. It also bears repeating that, “[a]lthough Plaintiff[] ha[s] sued Defendants in a single action, [her] claims against each Moving Defendant must be evaluated independently.” *Id.* at 12; *see also Mitchell*, 2014 WL 835129, at *6. Here, too, the Court concludes that Plaintiff is asking the Court to speculate as to the purposes of the Counties and their personnel in accessing her private data.

Plaintiff contends that “[her] Complaint goes far beyond mere speculation,” arguing that she

alleges that there is no legitimate law-enforcement reason for the [Counties'] personnel to obtain her information, her personal relationship with individual law enforcement officers, the gross number of “look-ups” and the fact that the [Counties'] personnel actually looked her up *by name*, should

lead this Court to infer that [the Counties] had no reason permitted under the DPPA to obtain [her p]rivate [d]ata.

(Pl.'s Mem. in Opp'n to Cnties. at 14, ECF No. 14.)

But, as discussed above, Plaintiff cannot simply lump together all of the alleged impermissible accesses; each defendant, and arguably each access, must be considered individually under the DPPA. And while Plaintiff continues to rely on her "contentious personal relationship with several police officers," (*id.* at 15), there are no allegations that *these* law enforcement officers are employed by the Counties.

Plaintiff attempts to distinguish her case from the *Kost* case, arguing that "[o]ne of the main distinctions is that [Plaintiff] has only sued over acts of obtaining her information by name lookup only, never by license plate number." (*Id.* at 15.) Plaintiff contends that

[a] random access, or any access of a license plate, may be for a legitimate purpose, for example that of ascertaining whether a car is not stolen. However, a name access will rarely if ever be for a law-enforcement purpose unless the person whose information has been accessed is under investigation or has reported a crime.

(*Id.* at 15.) *See Mallak*, 2014 WL 1285807, at *9 ("But, in [*Kost*], the plaintiff's information was searched by driver's license number; a search by driver's license number (as opposed to a search by name) reasonably implicates a number of legitimate law enforcement concerns."). While Plaintiff's private data may have been accessed by a different "search criteria" than the accesses that occurred in *Kost*, the manner in which the accesses were accomplished does not change the fact that Plaintiff must still sufficiently allege that her information was accessed for a purpose not permitted by the

DPPA. Notably, several courts in this District have considered cases in which the accesses were accomplished by name, rather than license plate number, and still concluded that the complaint lacked sufficient allegations to reasonably infer that that access was done for an impermissible purpose. *See, e.g., Ray*, No. 14-cv-539 (PAM/TNL) (Compl. ¶¶ 3, 4, 151, 231, ECF No. 1), 2014 WL 2511087, at *5; *Mitchell*, No. 13-cv-2167 (JNE/FLN) (Compl. ¶¶ 3, 137, ECF No. 1), 2014 WL 835129, at *6; *Bass*, No. 13-cv-860 (DSD/JJG) (Compl. ¶¶ 3, 265, ECF No. 1), 2014 WL 683969, at *3-4.

Plaintiff attempts to draw a parallel between the heft of the allegations needed to state a claim under the DPPA and the pleading of discriminatory intent in an employment discrimination case. (Pl.’s Mem. in Opp’n to Cnties. at 17.) Plaintiff argues:

One is not required to prove a *specific discriminatory intent* not only to avoid a motion to dismiss, but to prevail on a claim for employment discrimination, other than that the adverse employment action had as a contributing factor some discriminatory motive. . . . This is because no one can definitively prove what lies inside another’s mind; rather, one can prove that all other legitimate motives were not prevalent in making the employment decision.

(*Id.* at 16-17.) Plaintiff argues that “the same analysis should control” and her allegations are sufficient: “she was not implicated in any crime”; “the accesses were all by name”; “there was no legitimate law enforcement reason to access her by name”; “her name was well-known in the law-enforcement community due to her marriage to a law-enforcement officer and her contentious *personal* relationship with several members of law

enforcement”; “this status was related to many of the accesses”; and “none of the apparent reasons for accessing her by name appear[] to be present.” (*Id.* at 17.)

Whatever parallels, if any, could be drawn between pleading DDPA and employment discrimination claims, the allegations in Plaintiff’s Complaint do not permit the inferences Plaintiff would have the Court draw from her argument. There are no allegations that Plaintiff was “well-known in the law-enforcement community”—only that she was, at one point, married to a law enforcement officer. (*See* Compl. ¶¶ 52-55.) *Cf. Mallak*, 2014 WL 1285807, at *8 (“Additionally, Plaintiff alleges that she is a well-known attorney in her area with strong ties to the community.”); *Mitchell*, 2014 WL 835129, at *3 (describing allegations regarding Plaintiff’s celebrity as a local and national television news reporter and interviews with numerous law enforcement personnel). There are also no allegations that Plaintiff had “contentious *personal* relationships with several members of law enforcement.” The only relationship discussed, other than Plaintiff’s prior marriage, is the affair between Plaintiff’s ex-husband and Defendant Female Officer. (Compl. ¶¶ 54, 55, 71, 134.) Again, there are no allegations that any of these contentious relationships were with law enforcement officers employed by the Counties. The facts alleged simply “do not reflect an outward manifestation of the alleged impermissible purpose” of the Counties or their law-enforcement officers. *Mitchell*, 2014 WL 835129, at *6.

Plaintiff argues that requiring her to plead with further specificity at this stage in the proceedings is “impossible” because she does not know the names of the individual officers involved (outside of Defendant Female Officer, it would appear), which will be

revealed in discovery.¹¹ (Pl.’s Mem. in Opp’n to Cnties. at 13, 18.) The Court is not unsympathetic to Plaintiff’s argument that knowing the identity of the particular law enforcement officers who accessed her information may give her a stronger basis from which to plead that any particular access was for a purpose not permitted by the DPPA. And it may be the rare case in which a plaintiff is able to plead enough facts for a court to reasonably infer that the plaintiff’s information was knowingly accessed for an impermissible purpose. *See, e.g., Smythe*, 2013 WL 2443849, at *6; *see also Mitchell*, 2014 WL 835129, at *8 (listing cases that “generally included some indication of a connection or interaction between an identifiable law enforcement officer and the plaintiff, from which the asserted impropriety of the officer’s retrieval of the plaintiff’s data can be plausibly inferred”). But such a result is not inconsistent with the DPPA’s broad exception for use of such information by governmental entities, *see* 18 U.S.C. § 2721(b)(1); *Kost II*, 2013 WL 6048921, at *12; *Smythe*, 2013 WL 2443849, at *5, and the fact that the statute contains a separate remedy addressing the type of systemic abuse Plaintiff appears to be alleging, *see* 18 U.S.C. § 2723(b) (subjecting “[a]ny State department of motor vehicles that has a policy or practice of substantial noncompliance with this chapter” to civil penalties); *Kiminski*, 2013 WL 6872425, at *8.

¹¹ In this vein, Plaintiff asks the Court “to take judicial notice” of the *Rasmusson* case. (Pl.’s Mem. in Opp’n to Cnties. at 17.) Plaintiff appears to be arguing that, at one point, there was a court order in *Rasmusson* directing the identities of the law enforcement officers who accessed Rasmusson’s information to be released. (*Id.* at 18.) Plaintiff has not provided any further information regarding the court order or the circumstances of its issuance. In any event, it appears that, at least with respect to some defendants, the procedural posture in *Rasmusson* was different than the present case because those defendants answered the complaint, which is likely to account for why such discovery occurred.

Accordingly, for the reasons stated above, the Court concludes that Plaintiff has failed to state a DPPA claim against the Counties and their personnel and, therefore, recommends that the Counties' motion be granted with respect to Count I.

2. Section 1983 Claims

The Counties also move for dismissal of Plaintiff's § 1983 claims, asserting that DPPA violations are not actionable through § 1983 and Plaintiff has not alleged an actionable violation of her constitutional privacy rights. (Cnties.' Mem. in Supp. at 14-23; *see also* Cnties.' Reply at 6-7, ECF No. 74.)

a. DPPA

Plaintiff "incorporates by reference the arguments set forth in [her] Response to Dakota County's Motion to Dismiss" on the issue of whether the DPPA's statutory scheme is sufficiently comprehensive to supplant relief under § 1983. (Pl.'s Mem. in Opp'n to Cnties. at 31.) Thus, for the same reasons stated above, the Court concludes that Plaintiff has failed to state a § 1983 claim based on violations of the DPPA against the Counties and their personnel.

b. Constitutional Privacy Claims

Plaintiff also "incorporates by reference the [c]onstitutional arguments set forth in [her] Response to the [Commissioners'] Motion to Dismiss." (*Id.* at 31.) Having already concluded that Plaintiff does not have a reasonable expectation of privacy in the information allegedly accessed, it follows that Plaintiff cannot state a claim under § 1983 against the Counties and their personnel for a violation of her constitutional privacy rights.

c. *Monell* Claims

The Counties also argue that “Plaintiff cannot establish a *Monell* claim.” (Cnties.’ Mem. in Supp. at 14 n.8.) As the Court previously observed, there can be no *Monell* claim when the constitutional claims alleged fail. *Brockinton*, 503 F.3d at 674; *Mallak*, 2014 WL 1285807, at *13; *Bass*, 2014 WL 683969, at *6. Therefore, because this Court concludes that Plaintiff has failed to state a § 1983 claim against the Counties for violations of her constitutional rights, any *Monell* claims alleged by Plaintiff also must fail.

d. State Law Claims

Finally, the Counties assert that, to the extent that Plaintiff is attempting to bring a § 1983 claim for violations of state law, § 1983 is not available for this purpose. (Cnties.’ Mem. in Supp. at 23.) In Count II, Plaintiff brings a § 1983 claim against the individual law enforcement officers who accessed her private data, alleging, in relevant part, that the acts of these officers violated “the laws of the State of Minnesota.” (Compl. ¶ 216.) “[A]lleged violations of state laws, state-agency regulations, and even state court orders do not by themselves state a claim under 42 U.S.C. § 1983.” *Scheeler v. City of St. Cloud*, 402 F.3d 826, 832 (8th Cir. 2005) (quotation omitted); *see also Preston v. City of Pleasant Hill*, 642 F.3d 646, 650 (8th Cir. 2011) (“A plaintiff may not bring a state claim under the aegis of § 1983”); *Rasmusson*, 2014 WL 107067, at *9 (“[A]s noted by the Eighth Circuit, ‘a violation of state law, without more, does not state a claim under the federal Constitution or 42 U.S.C. § 1983.’” (quoting *Bagley v. Rogerson*, 5 F.3d 325, 328 (8th Cir. 1993) (citation omitted))). Thus, to the extent that Plaintiff’s Complaint can be

read as asserting § 1983 claims against the Counties and their personnel based on violations of state law, such claims also fail.

Therefore, for the reasons stated above, the Court concludes that Plaintiff has failed to state a § 1983 claim against the Counties and their personnel, whether based on the DPPA, constitutional privacy rights, or state law, and recommends that the Counties' motion be granted with respect to Counts II and III.

3. Invasion of Privacy

Like Dakota County, the Counties also move for dismissal of Plaintiff's common-law, invasion-of-privacy tort claim because "Plaintiff has no legitimate expectation of privacy in the information contained in her driver's license record." (Cnties.' Mem. in Supp. at 24.) Here, too, Plaintiff "incorporates by reference the arguments set forth in [her] Response to Dakota County's Motion to Dismiss." (Pl.'s Mem. in Opp'n to Cnties. at 31.)

For the reasons discussed above regarding Dakota County, the Court recommends that the Counties' motion likewise be granted with respect to Count VI because the alleged intrusions would not be highly offensive to a reasonable person and, consequently, Plaintiff has failed to state a claim for intrusion upon seclusion against the Counties and their personnel.

4. Statutes of Limitation

Finally, the Counties argue that all but one of Plaintiff's claims against the Counties are barred by the applicable statutes of limitation. (Cnties.' Mem. in Supp. at 24-37.) Because the actual access dates will not cure any of the substantive defects

identified in Plaintiff's claims against the Counties, the Court declines to address any arguments pertaining to statutes of limitation.

D. Duluth

Plaintiff's allegations against Duluth are similar in structure to her claims against the Counties and include the same three types of defendants: the entity, the entity's employees, and supervisors employed by the entity. (Compl. ¶¶ 23, 42, 44-46.) Plaintiff alleges that her private data was accessed by Duluth ten times. (*Id.* ¶ 70.)

Just as before, Plaintiff alleges that the impermissible accesses occurred by "view[ing her] Private Data from her State-issued driver's license including her home address, color photograph or image, date of birth, eye color, height, weight and driver identification number." (*Id.* ¶ 96.) Plaintiff alleges that these accesses occurred by entering her name into the database, "not her license plate number, to look up her private, personal information." (*Id.* ¶ 137.) Plaintiff alleges that these "accesses were impermissible, meaning that the Defendants had no law-enforcement reason for accessing the information. Defendants accessed the information for personal reasons completely unrelated to their position as law-enforcement officers." (*Id.* ¶ 95; *see also id.* ¶¶ 158, 188-90.) Plaintiff further alleges that Duluth's supervisors "should have monitored, prevented and stopped the unauthorized access [of Plaintiff's] information" by the Counties' employees. (*Id.* ¶ 139.) Plaintiff also alleges that the Duluth and their supervisors "permitted, condoned, or acquiesced in this illegal access to Plaintiff's private information, and knew or should have known that it was occurring." (*Id.* ¶ 145; *see also id.* ¶¶ 144, 192.)

In addition to these general allegations, Plaintiff provides more specific allegations with respect to one Duluth law enforcement officer—Defendant Female Officer. (*Id.* ¶ 43; *see also id.* ¶ 45.) Plaintiff alleges that her then-husband had an affair with Defendant Female Officer and, after learning of the affair, “[Plaintiff] confronted [Defendant Female Officer] about the affair on September 30, 2009.” (*Id.* ¶¶ 54, 55.) Plaintiff alleges that one of the Duluth accesses at issue “occurred on September 30, 2009. On information and belief, [Defendant Female Officer] accessed Plaintiff’s driver’s license information on September 30, 2009, the same day Plaintiff confronted [Defendant Female Officer] about the extra-marital affair with [Plaintiff’s] then-husband.” (*Id.* ¶ 71; *see also id.* ¶ 134.)

Duluth has moved to dismiss all claims asserted against it. Although the motion before the Court states that Duluth is moving for dismissal pursuant to Fed. R. Civ. P. 12(b)(6), Duluth acknowledges in its reply that “the motion is truly a motion for judgment on the pleadings under Rule 12(c), as the motion was filed after Duluth submitted an Answer to the Complaint.” (Duluth’s Reply at 1 n.1, ECF No. 76; Duluth’s Answer, ECF No. 26.) *See* Fed. R. Civ. P. 12(c) (“After the pleadings are closed—but early enough not to delay trial—a party may move for judgment on the pleadings.”). “Duluth respectfully requests that the Court treat this motion as if styled under Rule 12(c).” (Duluth’s Reply at 1 n.1.) “The same standard applies to a motion to dismiss for failure to state a claim under Rule 12(b)(6) and a motion for judgment on the pleadings under Rule 12(c).” *Kost II*, 2013 WL 6048921, at *2. Accordingly, the Court will consider Duluth’s motion under the standard identified at the beginning of this section.

1. DPPA

“Duluth joins and adopts the legal arguments for dismissal set forth in the [Counties’] recent memorandum of law in support of their motion to dismiss [P]laintiff’s DPPA claims for failure to state a claim,” including that the viewing of Plaintiff’s data without more is insufficient to state a DPPA claim and Plaintiff’s factual allegations do not permit the Court to infer plausibly that her private data was accessed for a purpose not permitted by the DPPA. (Duluth’s Mem. in Supp. at 3, ECF No. 51; *see also id.* at 5, 7-8; Duluth’s Reply at 4-5.) Duluth also argues that Plaintiff’s DPPA claim fails because she does not plead actual damages. (Duluth’s Mem. in Supp. at 3; *see also id.* at 6, 8.) Because of the additional allegations made with respect to Defendant Female Officer, the Court will address Duluth and Defendant Female Officer separately.

a. Duluth

The allegations comprising Plaintiff’s DPPA claim against Duluth are no different than the generic allegations discussed above with respect to Dakota County and the Counties. In fact, with respect to the city itself, there are no additional facts alleged distinguishing Duluth’s accesses from those of Dakota County and the Counties. As already discussed with respect to those defendants, the Complaint fails to state any facts that would permit the Court to reasonably infer that Plaintiff’s private data was accessed for a purpose not permitted by the DPPA. The same holds true for Duluth. “The complaint must . . . allege facts . . . that support an inference that [Duluth] knowingly accessed Plaintiff[’s] data for an impermissible purpose.” *Kost II*, 2013 WL 6048921, at

*11. Plaintiff has failed to do so and therefore the Court recommends that Duluth's motion be granted as to the city itself on Count I.

b. Defendant Female Officer

There is some question as to whether Duluth intends to move for judgment on the pleadings with respect to its employee, Defendant Female Officer. Duluth does not appear to recognize her as a party to this litigation, but at the same time makes arguments suggesting that its motion is intended to encompass her as well. (*See, e.g.*, Duluth's Mem. in Supp. at 2-3, 8, 9; Duluth's Reply at 1-2, 6-8.) To the extent that Duluth's motion can be read as seeking judgment on the pleadings with respect to Plaintiff's DPPA claim against Defendant Female Officer, the Court recommends that Duluth's motion be denied.

"Courts have found DPPA liability where an officer's retrieval of information was clearly for a personal purpose or for outright misuse." *Smythe*, 2013 WL 2443849, at *5. While the general allegations pleaded against Duluth itself do not permit the Court to reasonably infer that Plaintiff's private data was accessed for a purpose not permitted by the DPPA, the allegations against Defendant Female Officer permit the Court to reasonable infer that she accessed Plaintiff's information for a purpose not permitted by the DPPA and, therefore, plausibly state a DPPA violation. Here, there is "some indication of a connection or interaction between an identifiable law enforcement officer and the plaintiff, from which the asserted impropriety of the officer's retrieval of the plaintiff's data can be plausibly inferred." *Mitchell*, 2014 WL 835129, at *8. Plaintiff alleges she discovered that Defendant Female Officer, a Duluth employee, was having an

affair with Plaintiff's then-husband. After she became aware of the affair, Plaintiff confronted Defendant Female Officer about the affair. Plaintiff alleges that this confrontation took place on September 30, 2009, and at least one of the Duluth accesses at issue occurred on or about the same time. Taking these additional facts in the light most favorable to Plaintiff, alongside Plaintiff's allegations that the accesses at issue were accomplished by entering her name into the database and that there was no law enforcement purpose for the access, one could reasonably infer that Defendant Female Officer accessed Plaintiff's private data for some personal reason unrelated to law enforcement and for a purpose not permitted under the DPPA. *See Mallak*, 2014 WL 1285807, at *8, 9; *Smythe*, 2013 WL 2443849, at *5, 6.

Duluth argues:

These allegations ask the Court to assume a lot: that a Duluth police officer was in fact having an affair with [P]laintiff's ex-husband; that the officer (whom [P]laintiff by her own admission "confronted") was the same officer that subsequently accessed her information; that this same officer accessed [P]laintiff's driver's license information for personal reasons, versus a reason permitted under the broad law enforcement exception under the DPPA; that it is not permitted under the DPPA for a police officer to access the driver's license information of an individual who admittedly "confronts" them, and so on.

(Duluth's Reply at 6.) But, at least with respect to the existence of the extramarital affair, subsequent confrontation, and the chronological proximity between the confrontation and the look-up, the Court is required to take these alleged facts as true. *See Raynor*, 690 F.3d at 955. Moreover, the Court is to draw all reasonable inferences in favor of Plaintiff. *Id.* Plaintiff alleges that she has not committed any crimes and that there was

no law enforcement purpose behind the accesses. (Compl. ¶¶ 95, 159.) Under these circumstances, it is reasonable to infer that Defendant Female Officer, a Duluth employee, was behind the accesses of Plaintiff's information by a Duluth employee at or near the time that Plaintiff confronted a Duluth employee about an affair, and that the access was for a purpose not permitted by the DPPA. *See Smythe*, 2013 WL 2443849, at *6 (allegations that officer retrieved plaintiff's driver's license information for personal reasons and not for law enforcement purpose plausibly stated DPPA violation in light of parties' history). Duluth also appears to be suggesting that Plaintiff's confrontation could have been perceived as threatening to Defendant Female Officer and any subsequent access of Plaintiff's information would be likely permissible in response to a perceived threat to the law enforcement officer. While discovery may reveal support for this suggestion, dismissal at this stage on such a supposition is premature. *See id.* at *7, 8 (noting nature of parties' communications "may demonstrate [defendant officer] acted with or without a permissible purpose in retrieving [plaintiff's] motor vehicle records").

"In sum, Plaintiff puts forth sufficient allegations, when considered cumulatively, to 'raise a reasonable expectation that discovery will reveal evidence of [a DPPA claim]'" with respect to Defendant Female Officer. *Mallak*, 2014 WL 1285807, at *8 (alteration in original) (quoting *Twombly*, 550 U.S. at 556).

The Court makes one final comment with respect the allegations against Defendant Female Officer. As discussed above in III(B)(1), the Court cannot make a determination as to whether dismissal of Plaintiff's DPPA claims is warranted based on the statute of limitations because the dates of the alleged accesses cannot be determined

from the Complaint itself. *See Illig*, 652 F.3d at 976. At least with respect to Defendant Female Officer, however, it is clear that the September 30, 2009 access alleged fell within the four-year statute of limitations regardless of whether the four years is measured from the date of the access or the date Plaintiff learned of the access. *See, e.g., Rasmussen*, 2014 WL 107067, at *11 (applying general four-year statute of limitations under 28 U.S.C. § 1658(a) to DPPA claims); *Kost II*, 2013 WL 6048921, at *5 (same); *Smythe*, 2013 WL 2443849, at *6 n.13 (same).

c. DPPA & Damages

Because the Court finds that Plaintiff has stated a claim against Defendant Female Officer, the Court briefly addresses Duluth's argument that Plaintiff has not alleged "any actual damages flowing from the 10 purported viewings." (Duluth's Mem. in Supp. at 8; *see also id.* at 6.) Plaintiff responds that "[she] alleges actual damages—emotional distress, nervousness, tearfulness, physical illness, an inability to sleep and inability to eat—all resulting from Defendant's actions," and, in any event, Duluth's argument that "actual damages are a prerequisite to liquidated damages" under 18 U.S.C. § 2724(b)(1) is unavailing. (Pl.'s Mem. in Opp'n to Duluth at 14, 15, ECF No. 71.)

Section 2724 lists certain remedies a court may award in a civil action for violations of the DPPA. 18 U.S.C. § 2724(b). These include "actual damages, but not less than liquidated damages in the amount of \$2,500"; punitive damages; attorneys' fees and costs; and "such other preliminary and equitable relief as the court determines to be appropriate." *Id.* § 2724(b)(1)-(4). The Court need not address the pleading of actual damages, however, because, as other courts in this District have held, "the remedies

provision does not show that entitlement to actual or liquidated damages under 18 U.S.C. § 2724(b)(1) is a prerequisite for stating a claim upon which relief can be granted for a DPPA violation.” *Kost II*, 2013 WL 6048921, at *9; *accord Mallak*, 2014 WL 1285807, at *9 (“As articulated in *Kost*, the DPPA does not require a showing of entitlement to actual or liquidated damages as a prerequisite to state a valid claim upon which relief can be granted.”).

[T]he DPPA’s remedies provision includes a number of potential remedies that are discretionary for the court (“the court may award”), and a plaintiff can later choose which damages she seeks to prove at trial. Thus, at this stage, dismissal based on failure to plead actual damages is both premature and inappropriate.

Mallak, 2014 WL 1285807, at *9 (citation omitted).

Accordingly, with respect to Count I, the Court recommends that Duluth’s motion be granted in part with respect to Plaintiff’s DPPA claim against Duluth and denied in part with respect to Plaintiff’s DPPA claim against Defendant Female Officer.

2. Section 1983 Claims

With respect to Plaintiff’s § 1983 claims, both Duluth and Plaintiff economically incorporate by reference arguments stated elsewhere. “Duluth incorporates, as if fully set forth herein, the [Counties’] legal arguments for dismissal of [P]laintiff’s attempts to assert [§] 1983 claims against the individual and governmental entity defendants.” (Duluth’s Mem. in Supp. at 8-9.) Duluth writes separately only to state “that, to the extent that [P]laintiff is claiming that actions of an unnamed officer on September 30, 2009 resulted in a constitutional violation, isolated incidents of alleged constitutional

harm are insufficient to establish liability under [§] 1983 and *Monell*.” (*Id.* at 9 (citation omitted).) “Plaintiff incorporates by reference the Constitutional arguments set forth in Plaintiff’s Response to [the Commissioners’] Motion to Dismiss and Plaintiff’s Response to Dakota County’s Motion to Dismiss.” (Pl.’s Mem. in Opp’n to Duluth at 18 (citations omitted).)

For the reasons stated above with respect to the Commissioners, Dakota County, and the Counties, any § 1983 claim against Duluth based on violations of the DPPA fails because Plaintiff has failed to state a DPPA claim against Duluth. Moreover, the DPPA’s comprehensive enforcement scheme forecloses a § 1983 remedy for violations of the DPPA. Thus, the Court’s conclusion that Plaintiff has stated a DPPA claim against Defendant Female Officer does not save Plaintiff’s § 1983 claim premised on violations of the DPPA. Likewise, for the reasons stated above, Plaintiff does not have a reasonable expectation of privacy in the information allegedly accessed—which includes the information allegedly accessed by Defendant Female Officer—and therefore the access of such information cannot sustain a § 1983 claim for a violation of Plaintiff’s constitutional privacy rights. And, without any constitutional violation, any *Monell* claim necessarily fails. Lastly, to the extent that the Complaint can be read to assert a § 1983 claim for violations of state law, state-law violations by themselves do not state a claim under § 1983.

Accordingly, the Court recommends that Duluth be granted judgment on the pleadings with respect to Plaintiff’s § 1983 claims (Counts II and III).

3. Invasion of Privacy

The parties again take the same economical approach with respect to Plaintiff's invasion-of-privacy, common-law tort claim. Duluth incorporates the legal arguments of the Counties on this issue; Plaintiff incorporates the arguments made in response to Dakota County's motion to dismiss this claim. (Duluth's Mem. in Supp. at 10; Pl.'s Mem. in Opp'n to Duluth at 18.) For the reasons discussed above, the Court recommends that Duluth be granted judgment on the pleadings with respect to Count VI because the alleged intrusions would not be highly offensive to a reasonable person and, as a result, Plaintiff has failed to state a claim for intrusion upon seclusion against Duluth.¹² Because the intrusions at issue do not meet the requisite threshold of offensiveness, the Court declines to address the remainder of Duluth's arguments concerning the specificity of the allegations and timeliness of the claim. (*See* Duluth's Mem. in Supp. at 10.)

E. Cities

Similar to the other municipal defendants already discussed, Plaintiff's allegations against the Cities involve the Cities themselves and their personnel. (Compl. ¶¶ 20-22, 24-30, 32-37, 39-40, 42, 44-46.) And, with the exception of the actual number of accesses by the individual cities, Plaintiff's allegations against the Cities and their personnel are pleaded in the same manner as the other municipal defendants. Plaintiff alleges that the impermissible accesses occurred by "view[ing her] Private Data from her

¹² Duluth asserts that, "[a]s an initial matter, [P]laintiff's invasion of privacy claim is wholly dependent upon establishing a DPPA or [§] 1983 violation." (Duluth's Mem. in Supp. at 10.) The elements of an intrusion-upon-seclusion claim—an intrusion, which is highly offensive, into a matter in which a person has a legitimate expectation of privacy—do not require Plaintiff to establish a violation of federal statutory or constitutional law. *Swarthout*, 632 N.W.2d at 744.

State-issued driver's license including her home address, color photograph or image, date of birth, eye color, height, weight and driver identification number.” (*Id.* ¶ 96.) Plaintiff alleges that these accesses occurred by entering her name into the database, “not her license plate number, to look up her private, personal information.” (*Id.* ¶ 137.) Plaintiff alleges that these “accesses were impermissible, meaning that the Defendants had no law-enforcement reason for accessing the information. Defendants accessed the information for personal reasons completely unrelated to their position as law-enforcement officers.” (*Id.* ¶ 95; *see also id.* ¶¶ 158, 188-90.) Plaintiff further alleges that the Cities’ supervisors “should have monitored, prevented and stopped the unauthorized access [of Plaintiff’s] information” by the Cities’ employees. (*Id.* ¶ 139.) Plaintiff also alleges that the Cities and their supervisors “permitted, condoned, or acquiesced in this illegal access to Plaintiff’s private information, and knew or should have known that it was occurring.” (*Id.* ¶ 145; *see also id.* ¶¶ 144, 192.)

With respect to the Cities, there are 83 allegedly impermissible accesses at issue: Anoka (1), Burnsville (1), Eagan (2), Fremont (3), Farmington (3), Hancock (2), Lakeville (31), Mankato (2), Milaca (1), Morris (1), New Prague (1), Pequot Lakes (1), Richfield (3), Roseville (13), St. Francis (6), Staples (1), and the Dakota County Communications Center (11). (*Id.* ¶¶ 66, 67, 68, 72, 73, 74, 75, 77, 78, 79, 82, 83, 84, 87, 88, 89, 92; *see also id.* ¶ 136.)

1. DPPA

The Cities raise three primary arguments for dismissal of Plaintiff’s DPPA claims:

(1) Plaintiff “does not allege any facts to support a plausible inference [that] access to her

data fell outside of a law enforcement agency carrying out its functions or any other permissible use”; (2) the mere viewing of private data without more is not actionable under the DPPA; and (3) Plaintiff has failed to allege that she suffered actual damages as a result of the accesses. (Cities’ Mem. in Supp. at 5-20; *see also* Cities’ Reply at 2, ECF No. 77.) In particular, the Cities assert that Plaintiff’s DPPA claims “rest on ambiguous statutory language,” which

fails to provide a *clear* answer to two important questions: (1) whether a state or local official who merely searches or views driver’s license information—without disclosing or using it—has violated the DPPA (absent an authorized “purpose” for the search or view); and (2) whether someone who has failed to allege facts depicting actual damages caused by DPPA violations is still eligible for an award of “actual damages” against a state or local government or its officials.

(Cities’ Mem. in Supp. at 7, 8; *see also* Cities’ Reply at 8-11.) The Court leaves the adventures of statutory construction for another day as the Cities’ first argument is dispositive of Plaintiff’s DPPA claims.

As the Court has already stated multiple times, Plaintiff must allege facts regarding each of the Cities that would allow the Court to infer reasonably that a particular City knowingly accessed Plaintiff’s private data for a purpose not permitted by the DPPA. *Kost II*, 2013 WL 6048921, at *11. Plaintiff alleges the same facts against the Cities as she has against Dakota County and the Counties. Plaintiff offers no new arguments as to the sufficiency of the allegations pleaded, “incorporat[ing by reference] the arguments set forth in [her] Response to [the Counties’] Motion to Dismiss.” (Pl.’s Mem. in Opp’n to Cities at 23, ECF No. 73 (citation omitted).) These general allegations

“do not reflect an outward manifestation of the alleged impermissible purpose” of any of the Cities and their personnel. *Mitchell*, 2014 WL 835129, at *6.

The Court recognizes that the employment of Plaintiff’s then-husband by Defendant City of Lakeville provides an additional fact from which the Court *could* infer that the accesses by this defendant were for a purpose not permitted under the DPPA. Plaintiff, however, does not allege that she suspected her then-husband was accessing her data or that she had a contentious relationship with any of his coworkers. “[W]ithout some further factual enhancement[, Plaintiff’s Complaint] stops short of the line between possibility and plausibility of entitlement to relief.” *Twombly*, 550 U.S. at 557 (quotation omitted).

In sum, a complaint must do more than plead facts consistent with liability. *Id.* Plaintiff’s DPPA claims against the Cities fail for the same reasons already discussed with respect to the other municipal defendants and, therefore, the Court recommends that the Cities’ motion be granted with respect to Plaintiff’s DPPA claims (Count I).

2. Section 1983 Claims

As for Plaintiff’s § 1983 claims, the Cities raise the same arguments already addressed herein, namely that (1) Plaintiff’s driver’s license information “is not so extremely personal as to trigger constitutional privacy protection”; (2) Plaintiff has no reasonable expectation of privacy in the information allegedly accessed; and (3) DPPA violations are not actionable through § 1983. (Cities’ Mem. in Supp. at 27-31.) Plaintiff

relies on her prior responses to the Commissioners and Dakota County in opposing these arguments.¹³ (Pl.’s Mem. in Opp’n to Cities at 27.)

For the reasons already discussed above, the Court recommends that the Cities’ motion be granted with respect to Plaintiff’s § 1983 claims (Counts II and III) arising out of alleged violations of her constitutional privacy rights and the DPPA.¹⁴

3. Invasion of Privacy

The Cities also move for dismissal of Plaintiff’s common-law, invasion-of-privacy claims, arguing that “[Plaintiff] does not have a legitimate expectation of privacy in her driver’s license information because such information is routinely disseminated for a number of reasons,” and, “as a matter of law[, Plaintiff] cannot satisfy the ‘highly offensive’ prong” of an intrusion-upon-seclusion claim. (Cities’ Mem. in Supp. at 32.) This Court agrees and, for the reasons articulated above, the Court recommends that the Cities’ motion be granted with respect to Plaintiff’s invasion-of-privacy tort claims (Count VI).

4. Statutes of Limitation

Finally, the Cities argue that the majority of Plaintiff’s claims are barred by the applicable statutes of limitation. (*See, e.g., id.* at 20-27, 31 n.6, 32-33; Cities’ Reply at 3-8.) Because an analysis of the precise dates on which the alleged accesses occurred will

¹³ At one point in her response to the Cities’ motion, Plaintiff asserts that “Defendants, among others, so obtained and had access to information from [Plaintiff’s] driver’s license records, including her home address, date of birth, driver identification number, [S]ocial [S]ecurity number, and images and photos of her over time, as well as her height, weight, and eye color.” (Pl.’s Mem. in Opp’n to Cities at 4-5 (emphasis added).) Again, there are no allegations that Plaintiff’s Social Security number was disclosed in connection with any of the accesses in question. *See, e.g.,* discussion at III(A)(2)(b).

¹⁴ As previously noted, because the Court finds the absence of a reasonable expectation of privacy in driver’s license information to be determinative of Plaintiff’s constitutional privacy claims, the Court need not address whether the alleged accesses constitute a search under the Fourth Amendment. *See supra* n. 5.

not cure the substantive defects identified in Plaintiff's claims, the Court declines to address any arguments pertaining to statutes of limitation.

IV. LEAVE TO AMEND

Should the Court conclude that Plaintiff's claims are not sufficiently pleaded, Plaintiff requests leave to amend. (*See, e.g.*, Pl's Mem. in Opp'n to Dakota Cnty. at 43-44.) Plaintiff has neither filed a motion seeking leave to amend nor submitted a proposed amended pleading.

A party is permitted to amend its pleading once as a matter of course within 21 days "after service of a motion under Rule 12(b)." Fed. R. Civ. P. 15(a)(1)(B); *Thunander v. Uponor, Inc.*, No. 11-cv-2322 (SRN/SER), 887 F. Supp. 2d 850, 878 (D. Minn. 2012). Otherwise, "a party may amend its pleading only with the opposing party's written consent or the court's leave. The court should freely give leave when justice so requires." Fed. R. Civ. P. 15(a)(2). "Futility is a valid basis for denying leave to amend." *United States ex rel. Lee v. Fairview Health Sys.*, 413 F.3d 748, 749 (8th Cir. 2005). "[T]he Local Rules of this Court require a party seeking leave to amend a pleading to file a motion seeking such relief, accompanied by a copy of the proposed amended pleading." *Thunander*, 887 F. Supp. 2d at 879 (citing D. Minn. LR 15.1(b)).

Plaintiff has not formally moved to amend her Complaint. "A district court does not abuse its discretion in failing to invite an amended complaint when plaintiff has not moved to amend and submitted a proposed amended pleading." *Gomez v. Wells Fargo Bank, N.A.*, 676 F.3d 655, 665 (8th Cir. 2012) (quoting *Drobnak v. Andersen Corp.*, 561 F.3d 778, 787 (8th Cir. 2009)); accord *Mischia v. St. John's Mercy Health Sys.*, 457

F.3d 800, 805 (8th Cir. 2006) (district court did not abuse discretion in denying leave to amend where plaintiff requested leave “with a one line request in his brief opposing defendants’ motion to dismiss,” filed “no motion for leave to amend[,] and did not explain the substance of his proposed amendment”).

Further, any amendment is likely futile. For the reasons stated above, Plaintiff’s § 1983 and invasion-of-privacy claims (Counts II through VI) cannot be cured by way of amendment. As for Plaintiff’s DPPA claims (Count I), Plaintiff only addresses the replacement of Exhibit A to the Complaint with a corrected, “complete” audit. (Pl.’s Mem. in Opp’n to Dakota Cnty. at 43-44.) Notwithstanding the issues with Exhibit A, a more complete audit will not infuse the Complaint with factual allegations from which the Court could reasonably infer that a particular law enforcement officer’s access of Plaintiff’s information was for a purpose not permitted by the DPPA. Therefore, the Court recommends that Plaintiff’s informal request for leave to amend be denied at this time.

[Continued on next page.]

V. RECOMMENDATION

Based on the foregoing and all of the files, records, and proceedings herein, **IT IS HEREBY RECOMMENDED** that:

1. Commissioners Michael Campion and Ramona Dohman's Motion to Dismiss (ECF No. 19) be **GRANTED**.
2. County of Dakota's Motion to Dismiss (ECF No. 33) be **GRANTED**.
3. Motion to Dismiss of Defendants Isanti County, Mille Lacs County, Renville County, Rice County, Wright County and Yellow Medicine County (ECF No. 39) be **GRANTED**.
4. Defendant City of Duluth's Motion to Dismiss Pursuant to Fed. R. Civ. P. 8(a)(2) and 12(b)(6) (ECF No. 49) be **GRANTED IN PART** and **DENIED IN PART**.
5. Cities of Anoka, Burnsville, Eagan, Fairmont, Farmington, Hancock, Lakeville, Mankato, Milaca, Morris, New Prague, Pequot Lakes, Richfield, Roseville, St. Francis, and Staples and Dakota County Communications Center's Motion to Dismiss (ECF No. 53) be **GRANTED**.

Date: June 24, 2014

s/ Tony N. Leung
Tony N. Leung
United States Magistrate Judge
for the District of Minnesota

Loeffler v. City of Anoka et al.
Case No. 13-cv-2060 (MJD/TNL)

Pursuant to Local Rule 72.2(b), any party may object to this Report and Recommendation by filing with the Clerk of Court and by serving upon all parties written objections that specifically identify the portions of the Report to which objections are made and the basis of each objection. This Report and Recommendation does not constitute an order or judgment from the District Court and it is therefore not directly appealable to the Circuit Court of Appeals. Written objections must be filed with the Court before **July 9, 2014**.